Pázmány Péter Katolikus Egyetem

Jog- és Államtudományi Kar

Doktori Iskola

dr. NECZ Dániel

ÚJ FAJTA TUDÁS, ÚJ FAJTA HATALOM - A MESTERSÉGES INTELLIGENCIA ÉS A SZEMÉLYES ADATOK VÉDELME

doktori értekezés

A kézirat lezárva: 2024. május 04.

Témavezetők:

Dr. KOLTAY András (egyetemi tanár)

Dr. PÉTERFALVI Attila (címzetes egyetemi tanár)

Budapest, 2024

Édesanyámnak

Tartalomjegyzék

1. Bevezetés 5

2. A mesterséges intelligencia meghatározása, társadalmi szerepe 6

a. A mesterséges intelligencia meghatározása és története 7

b. A mesterséges intelligencia etikai alapjai és társadalmi hatásai 14

3. A mesterséges intelligencia szabályozása 18

a. A mesterséges intelligencia nemzetközi szabályozása 19

b. A mesterséges intelligencia szabályozása az Európai Unióban 28

c. A mesterséges intelligencia szabályozása az Amerikai Egyesült Államokban 48

d. A mesterséges intelligencia szabályozása az európai és amerikai szabályozáson túl 54

e. A technológiai nagyvállalatok önszabályozása 57

4. A mesterséges intelligencia általi adatkezelés az Európai Unióban 63

a. A személyes adatok és a mesterséges intelligencia 65

b. Az adatkezeléssel kapcsolatos szerepkörök a mesterséges intelligencia területén 73

c. A mesterséges intelligencia és az átláthatóság 72

d. A mesterséges intelligencia általi adatkezelés jogszerűsége 89

e. A mesterséges intelligencia és a különleges adatok kezelése 106

f. Az érintetti jogok gyakorlása 109

i. A tájékoztatáshoz és a hozzáféréshez való jog 111

ii. A helyesbítéshez és a törléshez való jog 114

iii. Az adatkezelés korlátozásához való jog 122

iv. Az adathordozhatósághoz való jog 124
v. A tiltakozáshoz való jog 128
vi. Az automatizált döntéshozatal és a profilalkotás 131
g. Az adatvédelmi és alapjogi hatásvizsgálat 134
h. A mesterséges intelligencia és az adatvédelmi tisztviselő 138
i. A mesterséges intelligencia és az adatbiztonság 142
j. A szektorális adatkezelés kihívásai 152
i. A mesterséges intelligencia szerepe az egészségügyben 153
ii. A mesterséges intelligencia munkahelyi alkalmazása 157
iii. A mesterséges intelligencia alkalmazása az online platformokon 162
5. A mesterséges intelligencia általi adatkezelés az Amerikai Egyesült Államokban 171
a) Az amerikai szabályozás 172
b) Az amerikai bírói gyakorlat 176
6. A mesterséges intelligenciával kapcsolatos különös adatvédelmi kihívások 179
a) Az általános célú mesterséges intelligencia 179
b) A deepfake technológia adatvédelmi kihívásai 184
c) A biometrikus azonosító rendszerek alkalmazása 189
7. A mesterséges intelligencia kapcsán szükséges-e újra gondolnunk a személyes adatok védelmét? 195
8. Záró gondolatok 201
9. Irodalomjegyzék 203

1. Bevezetés

Napjainkban az információ kiemelt értékkel bír, és az információs társadalom mozgatórugójává vált. Az információ ebben a kontextusban már nem csak az egyes szolgáltatásokhoz, tevékenységekhez kapcsolódó melléktermék, hanem a társadalom vagy a gazdaság, illetve egyes üzleti megoldások szervezésének alapja.[1] Mindemellett a digitalizáció és a technológiai fejlődés újabb vívmányai alkalmazásuk során jelentősen támaszkodnak napjaink adatalapú gazdaságára, amely így a személyes adatok tömeges gyűjtéséhez és elemzéséhez vezet. Például az arcképünk vagy a helyzetünk elemzése révén számos mesterséges intelligencia (MI) alapú alkalmazás képes pontosabb találati értékeket adni, és felhasználói igényeinket jobban kielégíteni. Mindennek oka, hogy az MI általában csak nagyfokú adatéhségének folyamatos kielégítése mellett fejleszthető tovább és alkalmazható sikeresen.

Az MI és a vele kapcsolatos társadalmi és gazdasági jelenségek azonban a személyiségi jogok, és ezen belül a személyes adatok védelmét is új kihívások elé állítják, lévén, hogy az MI általi, jellemzően tömegesen végzett adatkezelés számos olyan adatot érint, amely kapcsán, illetve amelyben személyek tömege bír változatos jogokkal és érdekekkel.[2] Ennek kapcsán sokan veszélyforrásként tekintenek az MI-re, amely egyben a személyes adatok védelmére is jelentős kockázatokkal bírhat. Vitathatatlan tény azonban, hogy az adatvédelem korábbi évtizedekben kimunkált alapelveinek, alapvető szabályainak és követelményeinek immár egy merőben új társadalmi, technológiai és gazdasági környezetben szükséges helytállnia, amely folyamatos újragondolást, és adott esetben nagyobb fokú rugalmasságot vár el a jogalkotótól és a jogalkalmazóktól. Ezen környezetben kérdésessé válik, hogy a magánszférába történő jelentősebb behatás okozta intenzívebb jogvédelem nem képezheti-e egyben gátját is a technológiai fejlődésnek, hátrányba hozva az Európai Uniót és annak tagállamait a technológiai versenyben a magánszférát jellemzően kevésbé védő rezsimekkel (például: Kínával) vagy a gazdasági verseny szabadságát különösen óvó Egyesült Államokkal szemben? Ugyanakkor kérdésként merül fel az is, hogy az átalakuló társadalmi és gazdasági környezetben nem szükséges-e a személyes adatok védelmét újra gondolnunk, és a technológiai fejlődés ívéhez, az egyes technológiák alkalmazásának sajátosságaihoz igazítanunk?

[1] Paolo GUARDA: „Free data?": open science in the age of personal data protection. In: Jacob H. ROOKSBY (ed.): *Research Handbook on Intellectual Property and Technology Transfer*. Cheltenham, Northampton, Edmund Elgar Publishing, 2020. 391.
[2] Chris REED: Data Trusts for Lawful AI Data Sharing. In: Gary Chan KOK YEW, Man YIP (eds.): *AI, Data and Private Law, Translating Theory into Practice*, Hart Publishing, 2021. 48.

A jelen értekezésben a fenti kérdésekre keressük a választ, a kodifikációs és technológiaszabályozási kérdések helyett adatvédelmi gyakorlati fókusszal. E körben kiemelt figyelmet fordítunk arra is, hogy a személyes adatok védelme hogyan garantálható a technológiai fejlődés támogatása, és így a versenyképesség megőrzése, valamint az adott technológia pozitív hatásainak kihasználása mellett, illetve, hogy a személyes adatok védelme hogyan biztosítható az MI sajátosságaira tekintettel. A fentieken túl az értekezésben jelentős figyelmet szentelünk az európai és amerikai szabályozás egyes vívmányainak, valamint sajátosságainak bemutatására. Ennek tükrében a részletes jogösszehasonlítástól eltekintünk, azonban figyelembe vesszük az egyes területek szabályozásának jellemzőit, és kitérünk az azokkal kapcsolatos lehetséges előnyökre és hátrányokra is. A fenti kérdések megválaszolásához azonban szükséges a főbb technológiai fogalmak tisztázása, társadalmi hatásainak és etikai szempontjainak, valamint a szabályozással kapcsolatos nehézségek ismertetése, amelyben a következő fejezetben kerítünk sort.

2. A mesterséges intelligencia meghatározása, társadalmi szerepe

Az MI fejlődése jelentős változásokat hozott magával, a digitális társadalom és gazdaság fejlődésével párhuzamosan. Ezen változások jelentős részben pozitívnak mondhatók, így napjainkra az MI-nek hála az interneten, illetve nagy méretű, ún. Big Data-adatbázisokból vagy akár számos, kisebb adatkészletből elérhető információ jelentős része könnyebben kereshetővé és feldolgozhatóvá vált, amely egyúttal számos tevékenység és feladat automatizált, valamint az emberinél hatékonyabb és gyorsabb elvégzéséhez is vezetett, az egyszerűbb, repetitívebb feladatoktól a komplexebb szakmai tudást igénylőkig.

Mindemellett azonban az MI elterjedése jelentős veszélyekkel is járhat a társadalom számára, valamint adott esetben alkalmas lehet arra, hogy a sérülékenyebb társadalmi csoportok tagjait (például: gyermekek, kiszolgáltatott helyzetben lévő személyek) negatívan befolyásolja. Így például gyermekek viselkedése is megfigyelhető egy okosjáték érzékelőin keresztül, amely aztán az információkat az azt forgalmazó vállalatnak továbbítja profilalkotás, szolgáltatásfejlesztés vagy marketingtevékenység támogatása érdekében.[3] Erre tekintettel vitathatatlan tény, hogy az MI alkalmazása számára egy olyan jogalkalmazási környezet

[3] Christoph BARTNECK, Christoph LÜTGE, Alan WAGNER, Sean WELSH: *An Introduction to Ethics in Robotics and AI*. Cham, Springer, 2021, eBook. https://doi.org/10.1007/978-3-030-51110-4. 68.

kialakítása szükséges, amelyben az új technológiai megoldások dinamikus módon fejleszthetők és hasznosíthatók, azonban az MI alkalmazásával járó káros hatások megelőzhetők vagy megfelelő időben és módon kiszűrhetők, így garantálva, hogy az MI fejlődése az emberiség további fejlődését megfelelően támogathassa.

Az alábbiakban az MI történetét és meghatározását, valamint etikai alapjait és társadalmi hatásait tekintjük át, annak érdekében, hogy az MI megoldások jelentőségét, sajátosságait, és ennek révén az MI szabályozás, valamint az MI általi adatkezelés számára kritikus szempontokat is megérthessük.

a. A mesterséges intelligencia meghatározása és története

A mesterséges intelligencia és a robotika története egészen az írott történelem hajnaláig nyúlik vissza. Az ókori Görögországban például több monda is napvilágot látott istenek alkotta mesterséges teremtményekről, ideértve például a Hésziodosz által feljegyzett Talos, a bronzból készült óriás történetét, akit Héphaisztosz isten hozott létre Kréta szigetének védelmére.[4] A mesterséges, ember módjára gondolkodó vagy viselkedő gépek iránti lelkesedés természetesen a későbbiekben sem lankadt. A felvilágosodás korának udvaraiban és szalonjaiban például a magyar feltaláló, Kempelen Farkas sakkozó gépe keltett szenzációt, amelyben azonban sajnálatosan valószínűleg emberi kezelő lapult. Később egyre inkább az irodalom és a filmipar foglalkozott az MI-vel, és különösen annak testet öltött formájával, a robotokkal.[5] Erre jó példának tekinthető Mary Shelley 19. század elején írt, Frankenstein című regénye, amely egy végül alkotója ellen forduló mesterséges teremtményt mutat be. Az emberek ellen forduló, fokozatosan öntudatra ébredő alkotások ezt követően is számos irodalmi mű és filmalkotás központi témája maradtak, ideértve például Karel Čapek 1920-ban bemutatott, R.U.R. című darabját, amely a szláv nyelvekből származó „robot" kifejezést is segített meghonosítani a köztudatban. A fentiek jó példának tekinthetők arra, hogy az MI megalkotása, fejlesztése révén az ember saját képére igyekszik segítőt alkotni magának.[6]

[4] Alex SHASHKEVICH: Stanford researcher examines earliest concepts of artificial intelligence, robots in ancient myths. *Stanford Report*, 2019.02.28. https://news.stanford.edu/2019/02/28/ancient-myths-reveal-early-fantasies-artificial-life/

[5] A mesterséges intelligencia irodalom- és filmtörténeti hivatkozásaihoz lásd: NECZ Dániel: A mesterséges intelligencia hatása a szerzői jogra. *Iparjogvédelmi és Szerzői Jogi Szemle*, 2018. 123/6. 52–53. [a továbbiakban: NECZ (2018)]

[6] UDVARY Sándor: Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései. Gazdaság és jog, 2018/12. 14.

Az MI kapcsán azonban az egyik leggyakrabban elhangzó, sokszor saját kontextusán túlmutató irodalmi hivatkozásnak a robotika három alaptörvénye tekinthető, amelyet az amerikai tudományos-fantasztikus író, Isaac Asimovhoz 1942-ben megjelent, Körbe-körbe című novellájában[7] fektetett le. Ennek értelmében tehát a robot

1. nem okozhat kárt embernek, és nem is tűrheti, hogy az kárt szenvedjék,
2. köteles engedelmeskedni az ember utasításának az első törvény sérelme nélkül,
3. köteles megvédeni saját magát az első két törvény sérelme nélkül.[8]

A mi részünkről a fenti három „alaptörvényt" alapvetően irodalmi hivatkozásnak tekintjük, mint jogi keretrendszernek, amely elsődlegesen a vonatkozó mű saját kontextusában értelmezhető, azonban ezen alaptörvények hatékonyan világítanak rá annak fontosságára, hogy az MI és a robotok szabályozott keretek között kerüljenek alkalmazásra, különösen, ha az adott megoldás az emberre is veszélyes lehet.

A számítógép és az informatika megalapozásának első lépéseit követően a huszadik század derekán az MI-vel kapcsolatos fejlesztések is különös lendületet vettek.[9] Ennek kapcsán kiemelt jelentőséggel bírt Warren McCulloch és Walter Pitts munkássága, akik az 1940-es években mesterséges genomokon alapuló elméletükkel sikeresen kimutatták, hogyan végezhetők számítások, illetve állíthatók elő függvények egymással összekötött genomok hálózatával.[10] Emellett az MI tudományos megalapozása és mérése kapcsán kiemelt jelentőségűnek tekinthető továbbá a híres angol matematikusról, Alan Turingról elnevezett, ún. Turing-teszt. Ennek alapjait Turing az 1950-ben megjelent „Számítógép és értelem" című tanulmányában fektette le. Ezen koncepció lényegében egy imitációs játékon alapul, amelyben egy „kérdező" és két

[7] A mű eredeti angol nyelvű címe: „Runaround", amely elsőként az Astounding című amerikai fantasztikus folyóirat 1942. márciusi számában jelent meg. Lásd: Isaac ASIMOV: Runaround. *Astounding Science-Fiction*, vol. 29 no. 1. (March 1942)

[8] Ennek kapcsán megemlítendő az adatvédelem és az átláthatóság szempontjából az Electronic Privacy Information Center (EPIC) elnevezésű nonprofit kutatóközpont korábbi elnökének, Marc Rotenberg-nek a javaslata a három asimovi törvény további két szabállyal való kiegészítésére: 4. törvény: a robot köteles a döntése alapját feltárni (algoritmikus átláthatóság), 5. törvény: a robot köteles személyiségét felfedni, illetve önmagát azonosítani. Lásd: Marc ROTENBERG: „Privacy in the Modern Age: The Search for Solutions". Marrakech (2016.10.19.): *38th International Conference of the Data Protection and Privacy Commissioners*. Elérhető: https://archive.epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf. 8.

[9] A mesterséges intelligencia tudománytörténeti előzményei kapcsán lásd: NECZ (2018) i. m. 53–55.

[10] ELEK István: *Az intelligencia spontán megjelenése*. Budapest, ELTE Eötvös Kiadó, 2015. 32–33.

másik „személy” vesz részt, egy ember és egy MI megoldás. A teszten akkor megy át a gépi válaszadó, vagyis az MI, ha elhiteti a kérdezővel, hogy ember.[11]

A fenti elméleti munkákat követően az 1950-es években jelentek meg az első, mai szóval MI-nek nevezhető megoldások. Így az évtized elején Christopher Strachey angol informatikus – részben Turing fenti művére, illetve iránymutatásaira támaszkodva – alkotott meg a Manchesteri Egyetem számítógépén egy programot, amely képes volt dámajátékot játszani, valamint egy adott szókészlet alapján szerelmesleveleket írni.[12] Emellett 1956-ban alkották meg Allen Newell, Herbert A. Simon és Cliff Shaw amerikai informatikusok a szintén elsők közé tehető MI alkalmazást, az ún. "Logic Theorist” elnevezésű programot, amely ugyanezen évben a Darthmouth Egyetemen megrendezett, első MI-ről szóló konferencián is bemutatásra került a tudományos nagyközönség számára.[13] Ezt követően egyre több olyan alkalmazás jelent meg, amelyek természetes nyelvi feldolgozásra (angolul: „*natural language processing*”) építenek. Ennek keretében lényegében az MI megtanul egy emberek által beszélt nyelvet, amelyen képes kommunikálni; e körben úttörőnek tekinthető Daniel G. Bobrow amerikai kutató doktori tanulmányai eredményeként 1964-ben létrehozott, STUDENT elnevezésű angol nyelvű algebra problémák megoldására tervezett MI megoldás.[14]

Nem sokkal a fenti kezdeti lépések után, 1966-ban jelent meg a Joseph Weinzbaum által készített, első chatbot alkalmazás, ELIZA is, amely egy pszichoterapeutával való beszélgetést imitált.[15] Ezt követte az 1972-ben, Kenneth Kolby pszichiáter által kifejlesztett, skizofrénekkel való beszélgetésre tervezett PARRY elnevezésű alkalmazás. A két alkalmazás egyébként 1972-ben „beszélgetett” is egymással, amelynek eredménye egy sok szempontból fura, szellemesnek mondható „társalgás” lett, amelyben szó esett többek között a szervezett bűnözésről és a szerencsejátékról is, amely iránt PARRY különösen nagy érdeklődést mutatott.[16] Ezt követően

[11] Alan Mathison TURING: Computing Machinery and Intelligence. *Mind*, vol. 59., no. 236. (October 1950) 433-434.
[12] Siobhan ROBERTS: Christopher Strachey’s Nineteen-Fifties Love Machine, *New Yorker*, 2017.02.14. https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine [2023.05.14.]
[13] Rockwell ANYOHA: The History of Artificial Intelligence, *Harvard SITN Blog*, 2017.08.28. http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/
[14] Daniel G. BOBROW: *Natural Language Input for a Computer Problem Solving System*. Cambridge, Massachusetts Institute of Technology, 1964.03.30, https://dspace.mit.edu/bitstream/handle/1721.1/5922/AIM-066.pdf?sequence=2&isAllowed=y. 4–6.
[15] ELIZA: a very basic Rogerian psychoterapist chatbot. https://web.njit.edu/~ronkowit/eliza.html
[16] Dylan LOVE: It Gets Pretty Weird When You Have Two ’Artificially Intelligent’ Chatbots Talk To Each Other. *Business Insider*, 2014.05.31. https://www.businessinsider.com/artificial-intelligence-chatbots-and-the-

1995-ben jelent meg a Richard Wallace szoftverfejlesztő által létrehozott, általánosabb célokra használható chatbot, Alice,[17] amelyet később a nagy technológiai vállalatok által fejlesztett, virtuális asszisztensek követtek, ideértve például a 2010-ben, az Apple által piacra vezetett SIRI, az Amazon által 2014-ben megjelentetett Alexa vagy a Microsoft által szintén 2014-ben megjelentetett Cortana elnevezésű alkalmazást. Ezek az alkalmazások rendkívüli népszerűségre tettek szert a felhasználók körében, akik a segítségükkel az adott vállalkozás termékeinek, szolgáltatásainak könnyebb elérésén, használatának támogatásán túl általános vagy hétköznapi kérdésekre is válaszokat kaphattak, továbbá akár szórakoztató társalgást is folytathattak az adott alkalmazással.

Hangsúlyozandó azonban, hogy az MI potenciális képességeit a kutatások ezen kezdeti időszakában jelentős kritikák is érték, megkérdőjelezve az MI valós tanulási képességeit. Erre jó példának tekinthető John Searle ún. kínai szoba érve (angolul: „*Chinese Room Argument*"). Ennek lényege, hogy amennyiben egy kínaiul egyáltalán nem tudó embert ültetnek egy szobába kínai nyelvű szövegekkel, és a szobán kívülről az általa értett nyelven adnak számára instrukciókat, valamint a válaszhoz szükséges további kínai szövegeket biztosítanak a számára, úgy a minták és az instrukciók alapján képes lesz a szövegeket párosítani, és kínai nyelven választ adni a kérdésekre anélkül, hogy ténylegesen értené a kínai nyelvet.[18] Értelemszerűen ez a logika alkalmazható az MI-re is, ideértve akár a manapság elterjedt, a korábbiaknál jóval fejlettebbnek számító alkalmazásokat is. Így ezen érv alapján egyesek könnyen juthatnak arra a következtetésre, hogy napjaink úttörőnek számító MI alapú megoldásai is inkább csak utánozzák az emberi értelmet, mintsem, hogy egy új, önálló intelligenciát képviselnének.

Az MI napjainkban tapasztalt rohamos fejlődése kapcsán szintén joggal merülhet fel bennünk a kérdés, hogy egy állandónak tekinthető fejlődési ívnek vagyunk-e tanúi vagy a jelenlegi fejlődési hullám inkább csak egy pillanatnyi „robbanásnak" tekinthető. Az ezredfordulót megelőző évtizedekre ugyanis inkább az „MI évszakok" váltakozása volt jellemző. Az 1950-es és 1960-as évek kezdeti lépéseit („MI tavaszát" vagy „MI nyarát") követően a 1970-es évekre az első „MI tél" köszöntött az emberiségre, amely beszűkült érdeklődéssel és fejlesztési

turing-test-2014-5?r=US&IR=T. Network Working Group, V. Cerf, PARRY Encounters the DOCTOR, 1973.01.21. https://datatracker.ietf.org/doc/html/rfc439

[17] Alice chatbot wins for third time. *BBC News*, last updated: 2004.09.20. http://news.bbc.co.uk/2/hi/technology/3672424.stm

[18] John R. SEARLE: Minds, brains, and programs. *Behavioral and Brain Sciences*, vol. 3., issue 3. (September 1980). doi:10.1017/S0140525X00005756. 417–419.

lehetőségekkel járt, majd az ezt követő újabb fellendülést követően az 1990-as évekre egy második „MI tél" köszöntött ránk[19]. Természetesen azonban ezen időszaknak is számos vívmányt köszönhetünk. Az 1980-as és 1990-es évekre például a személyi számítógépek megjelenésével és népszerűvé válásával összhangban egyre inkább elterjedtté váltak a különböző szakértői vagy tudás-alapú rendszerek, amelyek már kezdetleges MI-alapú megoldásokkal felvértezve voltak képesek támogatni a felhasználókat.[20] Ezt követően az MI még inkább rohamosnak tekinthető fejlődést könyvelhetett el. 1996-ben például a Deep Blue nevű számítógép legyőzte az akkori sakkvilágbajnokot, Garri Kaszparovot, 2011-ben pedig az IBM Watson elnevezésű természetes nyelvi feldolgozást alkalmazó megoldása győzedelmeskedett egy „Jeopardy" nevű kérdezz-felelek játékban.[21] A fejlődés egekbe szárnyaló íve napjainkra sem látszik megtörni. Az elmúlt időszakban például az OpenAI nevű nonprofit szervezet ChatGPT elnevezésű chatbot megoldása[22] vált a közfigyelem tárgyává, amely a felhasználókkal való hétköznapi társalgáson túl számos, sok esetben komplexnek tekinthető feladat elvégzésében képes segítséget nyújtani, ideértve például szövegfordítást, kutatómunka végzését, vagy épp programozást. A megoldás alkalmazása kapcsán azonban számos területen jogi és erkölcsi kérdések is felmerülnek, és jellemzően továbbra sem nélkülözhető az MI által végzett munka emberi felülvizsgálata. Erre egy new york-i ügyvédi iroda által 2023-ban elkövetett kínos hiba is rávilágított. Az iroda ügyvédjei egy légitársaság elleni per során olyan ügyekre hivatkoztak a beadványukban, amelyek nem léteztek. Mint kiderült, a kereseti kérelmük alátámasztásához precedensek keresésére használták a ChatGPT-t, amely sajnálatos módon nem létező, fabrikált ügyeket „talált" számukra, ezek pedig ellenőrizetlenül kerültek bele az iroda beadványába.[23]

Ami az MI meghatározását illeti, egyelőre nem beszélhetünk a szakirodalomban egységesen elfogadott definícióról, illetve minden tekintetben általánosan használt megközelítésről. A téma egyik úttörője, az amerikai kutató, John McCarthy az MI-t például az intelligens gépek, és különösen intelligens komputer programok létrehozásának tudományaként határozta meg.[24]

---

[19] Blagoj DELIPETREV, Chrisa TSINARAKI, Uroš KOSTIĆ: *AI Watch. Historical Evolution of Artificial Intelligence. Analysis of the three main paradigm shifts in AI*. Luxembourg, Publications Office of the European Union, 2020, doi:10.2760/801580. 3.
[20] DELIPETREV-TSINARAKI-KOSTIĆ op. cit. 9.
[21] DELIPETREV-TSINARAKI-KOSTIĆ op. cit. 13.
[22] ChatGPT, https://openai.com/blog/chatgpt
[23] Benjamin WEISER, Nate SCHWEBER: The ChatGPT Lawyer Explains Himself, *New York Times*, 2023.06.08, https://www.nytimes.com/2023/06/08/nyregion/lawyer-chatgpt-sanctions.html
[24] John MCCARTHY: What is Artificial Intelligence? Basic Questions. 2007.11.12. http://www-formal.stanford.edu/jmc/whatisai/node1.html

Ezzel szemben Elek István emberi módra, illetve logikusan gondolkodó gépek között tesz különbséget,[25] az MI céljaként pedig az intelligens entitások megértését és létrehozását jelöli meg.[26] Kiemelendő azonban, hogy az MI emberi intelligenciához való hasonlatosságát, valamint „emberihez" hasonló intelligencia létrehozásának lehetőségét több kutató is megkérdőjelezte, ideértve például Hubert Dreyfus amerikai filozófust is, aki az emberi módon való tanulás, illetve gondolkodás lehetőségének hiányában ragadta meg az MI fejlődésének korlátjait.[27].

A szakirodalmi meghatározásokon túl az MI és az ahhoz kapcsolódó egyes fogalmak napjainkra már jogszabályok, stratégiai dokumentumok, illetve nemzetközi egyezmények szövegeibe is utat találtak. Így például Magyarország Mesterséges Intelligencia Stratégiája az MI-t akként határozza meg „*mint a betáplált adatok alapján önmagukat tanítani és javítani képes algoritmikus rendszerek összessége*".[28] Hangsúlyozzuk azonban, hogy az MI meghatározásának valamennyi nemzetközi vagy nemzeti stratégiában, iránymutatásban vagy egyéb dokumentumban való megjelenésének feltérképezése és értelmezése túlmutatna a jelen tanulmány keretein, az ezzel kapcsolatos főbb szabályozási megközelítéseket azonban a tanulmány nemzetközi, európai uniós és amerikai szabályozást, valamint a technológiai nagyvállalatok önszabályozását tárgyaló részeiben ismertetjük.

Az MI történelmi és irodalmi előzményein, meghatározásán túl az MI alapvető működését is szükségesnek tartjuk áttekinteni, mivel ennek tükrében beszélhetünk csak a vonatkozó adatvédelmi problémákról. Mint ahogy fentebb is láthattuk, az MI-nek a gyakorlatban többféle meghatározása létezik, jellemzően olyan megoldásokat, technikákat értve ez alatt, amelyek a gépeket, programokat emberivé, működésüket az emberi gondolkodáshoz, megnyilvánulásokhoz hasonlóvá formálják; ennek egyik típusaként, illetve szorosan ehhez tartozó technológiaként tekinthető az ún. gépi tanulás (angolul: „*machine learning*"), amely olyan algoritmusok és statisztikai modellek kifejlesztését szolgálja, amelyeket számítógépek használnak emberi utasítások nélkül végzett műveletek elvégzésére, jellemzően meghatározott

[25] ELEK i. m. 22-23.
[26] ELEK i. m. 21.
[27] Hubert L. DREYFUS: *What Computers Still Can't Do. A Critical of Artificial Reason*. Cambridge, London, The MIT Press, 1992. 119.
[28] Innovációs és Technológiai Minisztérium: Magyarország Mesterséges Intelligencia Stratégiája 2020–2030, 2020, https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf. 6.

minták, korábbi tapasztalatok alapulvételével.[29] A gyakorlatban magát az „algoritmus" kifejezést is gyakran azonosítják az MI-vel vagy általában számítógépes programokkal, azonban ez a fenti kontextusban egy olyan utasítási rendszert jelent, amelyet a számítógép az adatokból való tanulás érdekében hajt végre.[30] A gépi tanulás egy gyakorlatban igen fejlettnek tekinthető módja az ún. mélytanulás (angolul: „*deep learning*"), amely esetén a tanulás és a feldolgozás sűrűn szőtt csomópontokból (angolul: „node") álló neurális hálózatokon valósul meg.[31] A neurális hálózatok esetén azonban az adatok feldolgozása, a tanulás során leírt súlyozása jellemzően annyira bonyolult, hogy számos esetben az ember által beláthatatlan, általunk fel nem ismert következtetésekhez vezethet.[32]

Az MI által kezelt adatok tekintetében a feldolgozás szakaszai alapján alapvetően bemeneti („*input*") és kimeneti („*output*") adatokat különböztethetünk meg, amelyeket az MI a rendeltetése szerinti célból felhasznál (input), majd ennek eredményeként létrehoz (output); ezen folyamat keretein belül is megkülönböztethetünk azonban valamely rendszerben aktívan tárolt és felhasznált adatokat („*production data*"), az ennek elemeit, tulajdonságait tükröző szintetikus adatokat („*synthetic data*"), valamint a kettő tulajdonságait ötvöző hibrid adatokat („*hybrid data*").[33] A fentebb írtakkal összhangban a bemeneti, illetve a kimeneti, valamint az MI működése során kezelt adatok közé személyes és nem személyes adatok, valamint kevert adatkészletek is tartozhatnak, amelyek kezelésére eltérő követelmények vonatkozhatnak. Szintetikus adatokat például gyakran használnak mesterségesen kreált, személyes adatoknak nem tekinthető információk létrehozására, amellyel adott esetben MI megoldások fejleszthetők, validálhatók, tesztelhetők, ekként például elkerülhető az adatvédelmi szabályoknak történő megfelelés, és könnyebben kiküszöbölhetők az adatkészlet szűkösségéből eredő problémák.[34] Az adatvédelmi jogszabályi rendelkezéseken túl továbbá egyéb jogszabályi rendelkezések is alkalmazhatók lehetnek az MI által kezelt adatokra, adatkészletekre vonatkozóan, ideértve

[29] AWS, What's the difference between AI and Machine Learning?, https://aws.amazon.com/compare/the-difference-between-artificial-intelligence-and-machine-learning/
[30] Kristian LUM, Rumman CHOWDHURY: What is an "algorithm"? It depends whom you ask. *MIT Technology Review*, 2021.02.26. https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/
[31] Larry Hardesty: Explained: Neural networks. *MIT News*, 2017.04.14. https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414
[32] CHRONOWSKI Nóra, KÁLMÁN Kinga, SZENTGÁLI-TÓTH Boldizsár: Régi keretek, új kihívások: a mesterséges intelligencia prudens bevonása a bírósági munkába és ennek hatása a tisztességes eljáráshoz való jogra. *Glossa Iuridica*, VIII/4. 2022. 15.
[33] Dario CASELLA, Laurence LAWSON: AI and privacy: Everything you need to know about trust and technology. *Ericsson*, 2022.08.01. https://www.ericsson.com/en/blog/2022/8/ai-and-privacy-everything-you-need-to-know
[34] Spanyol adatvédelmi hatóság (AEPD), Synthetic data and data protection, 2023.11.02, https://www.aepd.es/en/prensa-y-comunicacion/blog/synthetic-data-and-data-protection

például a szellemi tulajdonjogi, valamint személyiségi jogok védelmével, kibervédelemmel, fogyasztóvédelemmel kapcsolatos jogszabályi rendelkezéseket.

A fentieken túl megemlítendő, hogy az MI-t a gyakorlatban annak emberhez viszonyított képességei alapján gyakran csoportosítják továbbá szűk körű, általános, illetve szuper MI-re, amelyek közül az első kategóriára egy-egy adott feladat vagy feladattípus végzése kapcsán jól alkalmazható gyenge MI-ként, míg az utóbbi két kategóriára az ember képességeit elérő vagy azt túlszárnyaló, általánosan alkalmazható, erős MI-ként is hivatkozunk.[35] Míg gyenge MI-ből számtalan példát találunk szakértői vagy egy-egy egyszerűbb feladathoz használt MI-re, a nyilvánosság részéről a fokozott figyelem leginkább a jövőben esetlegesen kifejlesztett erős MI megoldásokat övezi. Ennek kapcsán mi úgy látjuk, hogy az MI-nek az ember kontrollja alatt kell maradnia, az azzal kapcsolatos felfokozott félelmek és „hype-szerű" hozzáállás azonban hátráltatja a technológia megfelelő kiaknázását és szabályozását. Az MI-vel kapcsolatos veszélyek és kockázatok álláspontunk szerint megfelelő szabályozás mellett racionális mértékben csökkenthetők, akár a mainál fejlettebb MI-rendszerek kifejlesztése és alkalmazása esetén is. Tekintettel azonban arra, hogy a jelen értekezés fókuszának az MI általi adatkezelés és a technológia adatvédelmi szempontjai tekintendők, így az értekezésben a különböző MI típusok sajátosságai helyett a továbbiakban az MI alkalmazásának adatvédelmi szempontjaira koncentrálunk. Emellett, az értekezésben ugyancsak főként az MI digitális megjelenésére fókuszálunk, és csak egyes adatvédelmi problémák ismertetése kapcsán térünk ki a robotok, mint „testet öltött" MI általi adatkezelésre.

b. A mesterséges intelligencia etikai alapjai és társadalmi hatásai

A fentebb írtakkal összhangban leszögezhető, hogy nem létezhet az emberiséget megfelelő módon szolgáló MI megfelelő etikai alapelvek figyelembevétele nélkül. Habár a sajtóban sokat idézett asimovi alapelvek a korábban írtak szerint főként irodalmi jelentőséggel bírnak, az azokban foglalt követelmények napjainkban is alapvető elvárásnak tűnhetnek az MI-vel szemben, ideértve különösen azon követelmény, hogy az csak az emberre, illetve az emberiségre nem veszélyes módon kerüljön alkalmazásra, jellemzően az ember döntésének, irányításának vagy felügyeletének alárendelten. Emellett reális elvárásnak tűnhet az is, hogy az MI önmagát is fejlessze, hogy „gazdájának", az embernek, illetve tágabb értelemben a

[35] IBM, AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?. https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/

társadalomnak, az emberiségnek is a hasznára váljék. Sajnálatosan azonban ezen általános érvényű elvek sem tekinthetők a gyakorlatban minden esetben alkalmazandónak. Így például már napjainkban is beszélhetünk olyan harci drónokról, amelyek bizonyos döntéseket saját maguk képesek meghozni. Az önvezérlő drónok elterjedése ennek kapcsán pedig akár még nagyobb veszélyekkel is járhat. A Future of Life Institute nevű szervezet például még 2017-ben készített egy „Slaughterbots" című, díjnyertes dokumentumfilmet, amely olyan kisméretű MI vezérelte drónokat mutat be, amelyek robbanószerrel vannak felszerelve, és méhkasként képesek akár nagyobb területek „elözönlésére", és a kiszemelt célpontok arcfelismerő rendszer útján való azonosítására, majd likvidálására.[36]

Megemlítendő továbbá, hogy a harctéren kívül is, egy-egy MI alkalmazás felett sokszor az alkotói csak korlátozott módon, illetve mértékben képesek kontrollt gyakorolni, amely magasabb fokú MI-rendszerek esetén már komolyabb kihívást jelenthet a társadalom számára. Még ugyanis a gyenge MI egy-egy feladat magas szintű ellátására, egy-egy korlátozott tevékenység végzésére képes,[37] addig az erős vagy általános MI már öntudattal bíró, általános intelligenciaként funkcionál, és képes az emberhez hasonló módon gondolkodni.[38] Mindez azonban értelemszerűen beláthatatlan következményekkel járhat, hiszen egy kiszámíthatatlan természetű, az emberivel vetekedő vagy azt meghaladó szintű értelem veszélyt is jelenthet az emberiség számára, és az ember legnagyobb segítőjéből legnagyobb riválisává válhat. Ugyanakkor ettől eltérő álláspontok is megismerhetők az MI-vel kapcsolatos szakirodalomban. Így Brian Christian technológiai kérdésekkel foglalkozó kutató az MI-ről írt The Most Human Human című könyvében hangsúlyozza például az MI azon tulajdonságát, amely szerint – a gépekhez hasonlóan – az MI saját célokkal vagy ehhez szükséges értékkészlettel vélhetően az intelligencia magasabb szintjén sem rendelkezne, így ennek tükrében a pusztító vagy az emberiséggel konkuráló erős MI képe is megkérdőjelezhető.[39] Ennek kapcsán megemlítendő, hogy a technológiai szektor területén is többen az MI-vel kapcsolatos veszélyek arányos és ésszerű kezelésére intettek az elmúlt években. A Microsoft technológiai nagyvállalat MI részlegének vezetője, Eric Boyd például 2023-ban a Sky News-nak adott interjújában kifejezetten az MI-ben rejlő lehetőségeket, pozitív társadalmi és gazdasági folyamatokat

[36] Henry BODKIN: Microdrones: the AI assassins set to become weapons of mass destruction. *The Telegraph*, 2022.11.14. https://www.telegraph.co.uk/global-health/terror-and-security/drone-assassins-micro-killing-machine/
[37] IBM, Strong AI vs. weak AI. https://www.ibm.com/topics/strong-ai
[38] Uo.
[39] Brian CHRISTIAN: *The Most Human Human*. New York, Anchor Books, 2011. 135-136.

hangsúlyozta, valamint azon álláspontját is kifejtette, miszerint az MI jelenlegi fejlettségi szintjén nem jelent veszélyt az emberiségre.[40]

Megemlítendő, hogy a 2010-es évek második felében az MI személyiségének kérdése is felmerült egy időre az európai jogalkotó részéről, amely jelentős vitákhoz vezetett. Az Európai Parlament például a Bizottságnak szóló, a robotikára vonatkozó polgári jogi szabályokról szóló 2017. januári jelentésében javasolta egyfajta korlátozott, „elektronikus személyiség" létrehozását azon helyzetekre, ahol a robotok önállóan döntenek vagy hasonlóan széleskörű autonómiát gyakorolnak.[41] A jelentésben foglaltakat, valamint a robotok jogalanyiságának gondolatát érthető módon számos kritika érte. Egy Európai Bizottságnak címzett levélben például több mint 150 szakértő fejezte ki aggodalmát a robotok jogalanyiságának elismerésével kapcsolatban, kiemelve többek között az MI által okozott kárral kapcsolatos felelősség erodálását.[42] Ezt követően az MI személyiségének kérdése „lekerült a napirendről", álláspontunk szerint helyesen. Az MI elvi értelemben gondolt „személyisége" ugyanis értelemszerűen nem tekinthető egyenlőnek az emberével, azzal egyezőként pedig nem értékelhető, kizárólag ahhoz hasonlítva vagy viszonyítva beszélhetünk róla. Kiemelendő továbbá, hogy ennél sarkosabb álláspontok is megjelentek a szakirodalomban, amelyek az MI-t és a robotokat az emberiség védelmében tartanák egyfajta jogfosztott vagy „jog nélküli" kategóriában. Így például Joanna J. Bryson kifejezetten akként fogalmaz, hogy a robotoknak az emberek szolgáinak kell maradniuk.[43]

A fentiektől eltekintve, és az MI képességeinek fejlődésére fókuszálva az utóbbi időben különösen a chatbotok, kép-, hang-, illetve videógeneráló szoftverek és egyéb hasonló nagy nyelvi modelleken (angolul: „*large langue models*", röviden: „*LLM*") alapuló MI-alapú megoldások területén figyelhetünk meg robbanásszerű fejlődést. A chatbot megoldások területén azonban a leginkább forradalminak tekinthető változást az OpenAI nonprofit szervezet által fejlesztett ChatGPT elnevezésű alkalmazás hozta el. A ChatGPT ugyanis a

[40] Tom CLARKE: Artificial intelligence 'doesn't have capability to take over', Microsoft boss says. *Sky News*, 2023.07.07, https://news.sky.com/story/artificial-intelligence-doesnt-have-capability-to-take-over-microsoft-boss-says-12916709
[41] Jelentés a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi ajánlásokról (2015/2103(INL)), A8-0005/2017, 2017.01.24. 19, 59(f) pont
[42] Politico, Open Letter to the European Commission, Artificial Intelligence and Robotics, https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf. 1.
[43] Joanna J. BRYSON: *Robots Should Be Slaves*. In Yorick Wilks (ed.): *Close engagements with artificial companions: key social, psychological, ethical and design issues*. John Benjamins Publishing Company, https://doi.org/10.1075/nlp.8.11bry

hétköznapi társalgáson túl számos, komplexebbnek tekinthető feladat elvégzésére is képes, ideértve – többek között – cikkek vagy elbeszélések írását, programozási vagy fordítási feladatok elvégzését. Jelentőségüket jól jelzi, hogy az utóbbi években már az online szerkesztőségek is számos alkalommal vesznek igénybe MI-alapú megoldásokat a napi hírekről vagy rendkívüli eseményekről tudósító, azokat összefoglaló cikkek írására, elkészítésére.[44] Természetesen a chatbot alkalmazásokon és a szöveges tartalmak generálás túl számos egyéb területet is forradalmasított az MI. A szintén OpenAI által fejlesztett DALL-E vagy a független Midjourney, Inc. kutatószervezet által létrehozott, Midjourney elnevezésű alkalmazás[45] napjainkban már képes például művészi vagy akár fotórealisztikus képek létrehozására is. Emellett az OpenAI 2024-ben beharangozott SORA elnevezésű alkalmazása képes akár filmminőségű videótartalmak készítésére is, amely számos területet új alapokra helyezhet, ideértve például a reklámipart vagy a filmipart is.[46]

A fentiekre tekintettel látható, hogy az MI, mint a digitális kor, és talán az emberiség legnagyobb vívmánya, a benne rejlő lehetőségeken túl egyben számos, korábban nem látott kihívás elé is állít minket. Mindez egyesek szerint egyfajta társadalmi megállapodás vagy konszenzus létrehozását követeli meg mind a nagyvállalatoktól, mind a nemzeti kormányoktól, valamint a társadalom egészétől az egyes MI alapú megoldások szabályozása kapcsán. A Microsoft vezérigazgatója, Satya Nadella például ennek kapcsán MI tervezési alapelvek, valamint iránymutatások létrehozását javasolta, ideértve például biztonsági és adatvédelmi szempontok figyelembevételét a technológiában rejlő bizalom erősítése érdekében.[47] Emellett Sam Altman, a ChatGPT megoldást kifejlesztő OpenAI intézet vezető tisztségviselője is nemrég nemzetközi együttműködésre és közös szabályozásra szólított fel az MI alapú megoldások fejlesztése területén.[48] Megemlítendő azonban, hogy az MI fejlesztések korlátozásával, felfüggesztésével kapcsolatos hangok is felerősödtek az utóbbi időszakban, amelyek a társadalom védelme szempontjából elengedhetetlennek tekintik az MI-alapú fejlesztések területén való „lassítást”. A 2018-ban elhunyt, neves angol matematikus, Stephen Hawking például a halála előtt az MI kontrolállhatatlan fejlődésével kapcsolatos veszélyekre,

[44] Böcskei BALÁZS, Német SZILVI: *Toxikus technokultúrák és digitális politika. Érzelmek, mémek, adatpolitika és figyelem az interneten*. Budapest, Napvilág Kiadó – TK PTI, 2021. 151.
[45] Midjourney, https://www.midjourney.com/
[46] OpenAI. Sora, https://openai.com/sora
[47] Microsoft, Democratizing AI: Satya Nadella on AI vision and societal impact at DLD, 2017.01.17, https://news.microsoft.com/europe/2017/01/17/democratizing-ai-satya-nadella-shares-vision-at-dld/
[48] Michelle TOH, Yoonjung SEO: OpenAI CEO calls for global cooperation to regulate AI. *CNN Business*, 2023.06.09. https://edition.cnn.com/2023/06/09/tech/korea-altman-chatgpt-ai-regulation-intl-hnk/index.html

és annak az emberiségre gyakorolt végzetes hatásaira hívta fel a figyelmet.[49] A közelmúltban továbbá számos szakértő, illetve vezető személyiség, például a techmilliárdos, Elon Musk, írt alá egy levelet, amely az MI fejlesztésekkel kapcsolatos lehetséges veszélyekre való reagálásként a GPT-4 modellnél fejlettebb MI-alapú megoldások fejlesztésének 6 hónapos felfüggesztésére szólított fel.[50]

A fentiek kapcsán álláspontunk szerint az MI-alapú fejlesztésekkel kapcsolatos korlátozásokra és szabályokra egyes kritikus területeken szükség van, általános fejlesztési korlátozás vagy tilalom bevezetése azonban aggályos lehet (ideértve például az olyan területeken, mint az egészségügyi kutatások), illetve egy ilyen korlátozás vagy tilalom az MI fejlesztésével és alkalmazásával járó pozitív és a negatív hatásokat egységesen is visszafoghatja. Erre tekintettel racionálisabb megoldásnak tűnhet az MI alapú fejlesztések pozitív hatásainak védelme, valamint az ilyen hatású, illetve irányú fejlesztések támogatása, míg a tilalmak és korlátozások útján kizárólag a negatív fejlesztési irányok, és hatások célbavétele. A fentiek kapcsán a túlzott protekcionizmus vagy egy-egy téma kapcsán való „hype-szerű" jogalkotói reakció, valamint a rövid-távú eredményeket előnyben részesítő szabályozás álláspontunk szerint kerülendő, ezek ugyanis jelentősen gyengíthetik az MI pozitív társadalmi, valamint gazdasági beágyazottságát. Az egyes területeken elterjedt szabályozási „homokozó" (vagy angol kifejezéssel: „*sandbox*") megoldások azonban kifejezetten hasznosak tűnnek, ezek ugyanis biztonságos keretet nyújtanak egy-egy innovatív megoldás kipróbálásához, mielőtt azok az adott piacon nyíltan kerülnének alkalmazásra. Ennek kapcsán jó példának tekinthetők az Európai Bizottság által, az ún. elosztott főkönyvi technológiák (angolul: „*Distributed Ledger Technologies*", röviden: „*DLT*") kapcsán 2023-ban bevezetett sandbox,[51] vagy az európai MI szabályozás kapcsán alább említett, nemzeti adatvédelmi hatóságok által bevezetett egyes sandbox programok.

3. A mesterséges intelligencia szabályozása

Az MI szabályozása kapcsán – az ennek szükségességét alátámasztó érveken túl – gyakran merülnek fel a technológiai és társadalmi fejlődés megakasztásának veszélyeivel kapcsolatos

[49] Rory CELLAN-JONES: Stephen Hawking warns artificial intelligence could end mankind. *BBC News*, 2014.12.02, https://www.bbc.com/news/technology-30290540
[50] Future of Life Institute, Pause Giant AI Experiments: An Open Letter, https://futureoflife.org/open-letter/pause-giant-ai-experiments/
[51] European Commission, Launch of the European Blockchain Regulatory Sandbox, 2023.02.14, https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox

kritikák, illetve az ettől való félelem. Ez lényegében ugyanannak a félelemnek az ellenpólusa, amely az MI-ben az emberi civilizációra jelentett legnagyobb veszélyt látja. Az MI azonban önmagában sem „megváltónak", sem „pusztítónak" nem tekinthető. Ehelyett álláspontunk szerint inkább egy olyan eszköz, amely megfelelő szabályozás mellett képes lehet az emberiséget méltó módon támogató technológiai megoldássá válni, ennek hiányában azonban jelentős veszélyekkel is bírhat, amely alól a személyes adatok kezelése, illetve azok védelme sem jelent kivételt.

A fentiekre tekintettel az értekezés jelen fejezetében az MI-vel kapcsolatos nemzetközi szabályozást, szabályozási törekvéseket, valamint a technológiai nagyvállalatok önszabályozását tárgyaljuk. Hangsúlyozzuk azonban, hogy a tanulmánynak nem célja a technológiaszabályozás részletekbe menő ismertetése, elemzése, tekintettel arra, hogy a dolgozatban az MI általi adatkezelésre és annak gyakorlati kihívásaira fókuszálunk, így az alábbi fejezetben kizárólag a főbb szabályozási irányvonalakat, önszabályozással kapcsolatos álláspontokat ismertetjük, amelyek egyben az MI általi adatkezelés egyes kihívásait is megjelenítik, illetve azok megértését is segítik.

a. A mesterséges intelligencia nemzetközi szabályozása

A fentebb előadottak tükrében látható, hogy az MI megfelelő szabályozási keretrendszert igényel ahhoz, hogy megfelelően legyen fejleszthető, illetve kerüljön alkalmazásra, a szabályozatlanságból eredő kockázatok minimalizálásával, valamint a negatív hatások lehetséges elkerülésével. Mindennek biztosításához azonban olyan szabályozási keretrendszer kialakítása szükséges, amely támogató az innovációval szemben, azonban igyekszik elejét venni a társadalom és az egyén jogait és érdekeit jelentős mértékben csorbító törekvéseknek, alkalmazási módoknak, és ahol az érintettek is megfelelően képesek saját kezükbe venni az irányítást, rendelkezni adataik megfelelő felhasználásáról.[52]

Az MI fejlődésével és elterjedésével kapcsolatos pozitív hatásokat nehéz vitatni, ezek napjainkra a társadalom, illetve a gazdaság szinte valamennyi területén, illetve számos szintjén megmutatkoznak. A virtuális asszisztensek, chatbotok segítségével könnyebbé válhat az

[52] PÓK László Gábor: Védeni vagy megosztani? – A személyes adatok szerepe az internetes platformok szabályozásában. In: TÖRÖK Bernát, ZŐDI Zsolt (szerk.): *Az internetes platformok kora*. Budapest, Ludovika Egyetemi Kiadó, 2022. 397. [a továbbiakban: PÓK (2022)]

ügyintézés, valamint egyes egyszerűbbnek tekinthető hétköznapi feladatok elvégzése, míg például a szociális és egészségügyi robotok sok szempontból javíthatnak az egészségügyi és szociális ellátáson. A fentieken túl számos egyéb MI-alapú, illetve MI-vel kapcsolatos innováció is hatalmas lehetőségekkel kecsegtet, ideértve például az önvezető autókat, amelyek képesek lehetnek biztonságosabbá tenni a közlekedést, valamint hatékonyabbá az áruszállítást. Az új technológiák, így különösen az MI, valamint az MI által feldolgozott jelentős adatmennyiség emellett önmagukban is katalizáló hatással bírnak a tudományos fejlődésre, kiemelt mértékben hozzájárulva ahhoz.[53] A fenti innovációk, új technológiák, megoldások alkalmazása azonban bizonyos veszélyekkel, illetve kockázatokkal is járhat, ideértve például az emberi kontroll elvesztését és a nem megfelelő technológiahasználatból eredő egyéb károkat, valamint az emberi munkaerő és kreativitás háttérbe szorítását. Az MI-vel kapcsolatos biztonsági kockázatok jelentőségét jól jelzi, hogy az Egyesült Nemzetek Szervezete (ENSZ) Biztonsági Tanácsa nemrégiben története során először tartott ülést az MI nemzetközi békére és biztonságra jelentett veszélyeinek témájában.[54] Emellett kiemelt jelentőséggel bírnak a különböző MI alkalmazással és fejlesztéssel kapcsolatos alapelveket és alapvető elvárásokat meghatározó nemzetközi törekvések, amelyek a nemzeti szabályozás, valamint a technológiai nagyvállalatok önszabályozásának is keretet adnak.

A fentiekre tekintettel az MI nemzetközi szabályozása kapcsán különös jelentőséggel bírnak a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) 2019. májusában elfogadott MI Alapelvei, [55] amelyek az MI értékalapú irányelveit határozzák meg, valamint további hasznos ajánlásokkal szolgálnak a szabályozók számára. Így ezen dokumentum az alábbi értékalapú irányelveket határozza meg:

- beleértett növekedés, fenntartható fejlődés és jólét,
- emberalapú értékek és tisztesség,
- átláthatóság és megmagyarázhatóság,
- átfogó jelleg, biztonság és védelem,
- elszámoltathatóság.[56]

[53] Mark OWEN, Maria LUCHIAN: Following the AI path. *Intellectual property magazine*, 2044-7175. (September 2020). 15.
[54] Edith M. LEDERER: UN council to hold first meeting on potential threats of artificial intelligence to global peace. *AP News*, 2023.07.03, https://apnews.com/article/artificial-intelligence-un-security-council-meeting-uk-f7fb6d8f8a261a9d9b23ca463ee29d3d
[55] OECD, AI Principles, https://oecd.ai/en/ai-principles
[56] OECD, AI Principles, 7-8.

Mindezen megközelítés egyben szintén az MI emberi értékekre tekintettel lévő, átlátható, biztonságos és elszámoltatható alkalmazását helyezi előtérbe, valamint hitet tesz a fenntartható fejlődés mellett, ugyanis az MI csak ennek keretein belül fejleszthető és alkalmazható biztonságos és etikus módon. Mindez azért is fontos, mivel az átláthatóság a gyakorlatban különös kihívást jelent az MI általi és egyéb komplex technológiák által végzett adatkezelések esetén, főként arra tekintettel, mivel a nagy technológiai vállalatok számára jellemzően elképesztően nagy mennyiségű személyes adat áll rendelkezésre, amelynek felhasználása jelentős számú adatkezelési cél megvalósítása érdekében történik.[57] Így a fenti alapelveknek való megfelelés keretet biztosíthat a személyes adatok MI általi kezelése tekintetében, amelyet a megfelelő szabályozás és gyakorlati alkalmazás tehet teljessé.

A fenti alapelveken túl az MI Alapelvek az alábbi ajánlásokat határozzák meg a szabályozók számára:

- befektetés az MI-alapú kutatásokba és fejlesztésekbe,
- digitális ökoszisztéma kiépítése az MI számára,
- az MI szabályozási környezetének létrehozása és lehetővé tétele,
- emberi erőforrás fejlesztése és a munkaerőpiaci átállásra való felkészülés,
- a megbízható MI-vel kapcsolatos nemzetközi együttműködés.[58]

A fentiekre tekintettel tehát az MI Alapelvek hangsúlyozzák a kutatás- és fejlesztés támogatásának jelentőségét az MI területén, valamint az MI-ben rejlő lehetőségek kiaknázásához szükséges megfelelő digitális környezet kialakítását, az emberi erőforrásokat, valamint a képzést és a megváltozott munkaerőpiaci viszonyokra való megfelelő és dinamikus reagálást, továbbá – tekintettel a technológia jellemzően határokat nem ismerő természetére – a nemzetközi együttműködést. Ezen utóbbi pont természetesen azért is fontos, mivel a nemzetek saját elszigetelt elvek és megközelítések mentén nem lehetnek képesek sikeres MI szabályozás kialakítására. A sikeres nemzeti vagy regionális szabályozásnak ugyanis amellett, hogy az etikus MI-vel kapcsolatos nemzetközileg elfogadott alapelveken kell nyugodnia, reagálnia kell az adott régió, környező államok és a nemzetközi közösségek által széleskörben elfogadott és alkalmazott szabályozási megoldásokra is. Mindezek hiánya ugyanis technológiai és gazdasági elszigetelődéshez vezethet.

[57] Omer TENE, Jules POLONETSKY: A Theory of Creepy: Technology, Privacy and Shifting Social Norms. *Yale Journal of Law & Technology*, vol. 16., no. 59. (2013) 71.
[58] OECD, AI Principles, 8-9.

Az Egyezmény a Mesterséges Intelligenciáról, az Emberi Jogokról, a Demokráciáról és a Jog Uralmáról („**ET Egyezmény**”)[59] az MI alkalmazásával kapcsolatban számos követelményt, valamint szempontot határoz meg, ideértve az MI hatóságok általi, valamint a termékértékesítés és szolgáltatásnyújtás során történő felhasználását. Emellett az ET Egyezmény meghatározza az MI tervezés, fejlesztés és alkalmazás alapelveit, az ezzel kapcsolatos szükséges intézkedéseket és garanciákat, valamint a nemzetközi együttműködéssel, és a hatóságok eljárásával kapcsolatos követelményeket.

Az ET Egyezmény a hatóságok általi MI felhasználás kapcsán hangsúlyozza az emberi jogi követelmények, valamint a demokratikus társadalmak által megkövetelt jogi és etikai elvárások figyelembevételét, e körben az emberi jogok és alapvető szabadságok megsértésének elkerülésére törekvést; emellett az ET Egyezmény hangsúlyozza az MI demokratikus intézmények általi, a jog uralmára tekintettel való alkalmazásának fontosságát, az MI szükséges és arányos alkalmazását, valamint a lehetséges kockázatok felmérését, ezzel kapcsolatban megfelelő intézkedések megtételét.[60]

Az MI termékértékesítés, valamint szolgáltatásnyújtás során történő felhasználása kapcsán az ET Egyezmény szintén hangsúlyozza az ezen tevékenységek emberi jogi követelményekre, valamint a demokratikus társadalmak elvárásaira, vonatkozó jogszabályi követelményekre tekintettel történő végzését, az emberi jogok és alapvető szabadságok, valamint a demokratikus társadalmi működés megsértésének elkerülésére törekvést. Emellett a fentiek kapcsán az ET Egyezmény kiemeli az MI alkalmazás vonatkozásában a közéleti vitákhoz való egyenlő és tisztességes hozzáférés fontosságát, valamint a közegészségügy és a környezet védelmét.[61]

A fentebb írtak szerint továbbá az ET Egyezmény az MI rendszerek tervezésének, fejlesztésének és alkalmazásának kapcsán is alapelveket határoz meg, ideértve

- az egyenlőség és diszkrimináció-ellenesség elvét,
- az adatvédelem és a személyes adatok védelmének elvét,
- az elszámoltathatóság, felelősség és jogi felelősségre vonhatóság elvét,

[59] Európa Tanács, Egyezmény a Mesterséges Intelligenciáról, az Emberi Jogokról, A Demokráciáról és a Jog Uralmáról, https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f
[60] ET Egyezmény, 5-6.
[61] ET Egyezmény, 6.

- az átláthatóság és a felülvizsgálat elvét,
- a biztonság elvét,
- a biztonságos innováció elvét.[62]

A fentieken túl az ET Egyezmény hangsúlyozza a nyilvános konzultáció fontosságát az MI rendszerek tervezésének, fejlesztésének és alkalmazásának kapcsán, valamint a kiemelt fontosságú kérdések megfelelő társadalmi vitának való alávetését.[63] Emellett az ET Egyezmény szintén kiemeli a megfelelő intézkedések és garanciák fontosságát, ideértve megfelelő jogorvoslati lehetőségek biztosítását, az érintettek részére ezek átlátható kommunikálását és az esetleges panaszok nyomon követhetőségét, illetve megköveteli további eljárási garanciák alkalmazását, e körbe értve az emberi felülvizsgálat lehetőségét az emberi jogokat és alapvető szabadságokat érintő lényeges információkat nyújtó vagy döntést hozó MI rendszerek esetén, továbbá a kapcsolódó emberi kommunikációt, valamint hatékony hozzájutást a vonatkozó garanciákhoz és lehetőségekhez.[64]

Az ET Egyezmény a fentiek mellett szintén különös hangsúlyt fordít a kockázatkezelésre, valamint a hatásvizsgálatra, tekintettel arra, hogy ezek különös jelentőséggel bírnak az MI-rendszerek jelentős részének alkalmazása kapcsán, különösen ideértve azon rendszereket, amelyek alkalmazása az egyénre és a demokratikus társadalmakra különös hatással bír. Így e körben az ET Egyezmény megköveteli a részes felektől egyértelmű iránymutatás kibocsátását a kockázatkezelés, valamint a hatásvizsgálat területén, az emberi jogokkal, a demokratikus társadalom működésével, valamint a jog uralmának betartásával, az ezekkel kapcsolatos esetleges károk és veszélyek elkerülésével kapcsolatban.[65] Mindemellett az ET Egyezmény szintén hangsúlyozza az MI-vel, a kapcsolódó kockázatokkal és hatásokkal kapcsolatos képzések fontosságát,[66] valamint a nemzetközi együttműködést és a nemzeti hatóságok megfelelő és demokratikus eljárását, erőforrásokkal való ellátását.[67]

A fentiek mellett nemzetközi szintén megemlítendő a Globális Együttműködés az MI Területén (angolul: „*Global Partnership on Artificial Intelligence*”; „*GPAI*”),[68] amelynek célja az MI-

[62] ET Egyezmény, 6-7.
[63] ET Egyezmény, 7.
[64] ET Egyezmény, 8.
[65] ET Egyezmény, 9.
[66] Uo.
[67] ET Egyezmény, 9-10.
[68] GPAI, https://gpai.ai/about/

rendszerek fejlesztésével és alkalmazásával kapcsolatos kockázatok azonosítása, valamint a kutatás- és fejlesztés, a megbízható MI-rendszerek elterjedésének támogatása. Az együttműködéshez eddig 29 ország csatlakozott, ideértve többek között az Egyesült Államokat, Kanadát, az Európai Uniót, Németországot, Franciaországot, valamint több egyéb európai, afrikai, ázsiai, valamint óceániai országot is (például: Japán, India, Ausztrália, stb.).

A nemzetközi szabályozás szempontjából szintén kiemelkedőnek tekintendők a G7 2023. őszi hiroshimai csúcstalálkozót követően kiadott, fejlett MI-rendszereket fejlesztő és alkalmazó vállalkozások részére szolgáló irányadó irányelvek (angolul: „*Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI*"), valamint az ezen szervezetek részére kiadott etikai kódex (angolul: „*Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems*").[69] A fenti alapelvek az olyan fejlett MI-rendszerek kapcsán határoznak meg alapvető követelményeket, mint a kiemelt jelentőségű MI-modellek (angolul: „*foundation model*") vagy a generatív MI-rendszerek, és magukban foglalják – többek között – a rendszerek alkalmazásával kapcsolatos kockázatok csökkentését, valamint az esetleges sebezhetőségek kivizsgálását, az incidensek szükséges körű hatósági jelentését, az átlátható alkalmazást, valamint megfelelő információbiztonsági és egyéb intézkedések megtételét.[70] Az etikai kódex a fenti irányelvek szerint határozza meg a fejlett MI-rendszereket fejlesztő és alkalmazó szervezetek alapvető követelményeit, és különösen hangsúlyozza a jog uralmát és az emberi jogokat, alapvető elveket tiszteletben tartó, emberközpontú MI-rendszerek tervezését, fejlesztését és alkalmazását.[71] A fenti hiroshimai irányelveket és kapcsolódó alapvető követelményeket a G7 vezetők 2023. december 6-i ülésükön is megerősítették, ahogy a GPAI, valamint a Data Free Flow with Trust (DFFT)[72] alapvető célkitűzéseinek fontosságát is, jól jelezve az adatok szabad áramlásának, digitális gazdaságok fejlődésének globális fontosságát és a velük kapcsolatos nemzetközi konszenzust, az MI ezzel kapcsolatos szerepét és jelentőségét.[73]

---

[69] The White House, G7 Leaders' Statement on the Hiroshima AI Process, 2023.10.30, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/

[70] Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI, https://www.mofa.go.jp/files/100573471.pdf

[71] Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, https://ec.europa.eu/newsroom/dae/redirection/document/99641

[72] A G20-ak 2019-es oszakai csúcstalálkozóján előirányzott követelmények, amelyek lehetővé tennék az adatok nemzetközi továbbításával kapcsolatos korlátozások lebontását. Lásd: Digital Agency, Data Free Flow with Trust (DFFT), https://www.digital.go.jp/en/dfft-en/

[73] The White House, G7 Leaders' Statement, 2023.12.06, https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/06/g7-leaders-statement-6/

Az MI-vel kapcsolatos nemzetközi előírások azonban, habár az MI nemzetközi szabályozása kapcsán előrelépést jelentenek, azonban sok szempontból általánosan fogalmaznak, ideértve az emberi jogi követelmények MI-rendszerekkel kapcsolatos konkrét megjelenítését is.[74] Erre tekintettel jelentőségük sokszor csak később, azokra hivatkozó regionális vagy nemzeti jogszabályokban, illetve az MI-vel kapcsolatos alapvető követelmények, elvárások formálódásában érhető tetten.

A fejlett MI-rendszerekkel kapcsolatos nemzetközi figyelmet és félelmeket jól jelzi továbbá a 2023. novemberi AI Safety Summit rendezvényen elfogadott Bletchley Declaration elnevezésű nyilatkozat,[75] amely több konkrét alkalmazási területet is nevesít, valamint hangsúlyozza az ilyen rendszerekkel való visszaéléssel és a nem megfelelő biztonsági intézkedések alkalmazásával kapcsolatos kockázatokat, ideértve például a biotechnológiai megoldások alkalmazásából származó esetleges károkat vagy a dezinformációt. A nyilatkozat továbbá hangsúlyozza a nemzetközi együttműködés, valamint a kockázatalapú megközelítés fontosságát, amely az MI-rendszerek által jelentett kockázat súlya szerinti szabályozást, illetve intézkedések alkalmazását teszi indokolttá. A nyilatkozat célkitűzései közé tartozik továbbá az MI-rendszerek alkalmazásával kapcsolatos közös, tudományos és kockázat-alapú megközelítés kialakítása, amely segítené az MI-szabályozás egységességét, valamint az ilyen rendszerek fejlesztőivel, szolgáltatóival szembeni arányos szabályozási és biztonsági követelmények támasztását.

A fentieken túl megemlítendő továbbá, hogy a közelmúltban az Európa Tanács keretein belül megszületett a mesterséges intelligenciáról, emberi jogokról, demokráciáról és a jog uralmáról szóló keretegyezmény tervezete is. Ezen dokumentum hangsúlyt helyez az adatvédelmi megfelelésre is, és valamennyi részes féltől elvárja az MI-rendszerek teljes élettartama alatt az érintett személyek személyes adatai védelmének biztosítását, valamint megfelelő biztosítékok és garanciák alkalmazását,[76] ezzel is hangsúlyozva a személyes adatok védelmének fontosságát az MI fejlesztése és alkalmazása területén.

[74] Lottie LANE: Clarifying Human Rights Standards Through Artificial Intelligence Initiatives. *International and Comparative Law Quarterly*, vol. 71., issue 4. (2022) 941. [a továbbiakban: LANE (2022)]
[75] The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023, 2023.11.01, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023
[76] Council of Europe, Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680aee411. Article 11.

A fenti nemzetközi szabályozási törekvések természetesen a regionális, valamint a nemzeti MI szabályozás számára is kereteket, valamint etikai és szabályozási alapelveket biztosítanak, egyben szabályozási konszenzust és minimumkövetelményeket is megjelenítenek a demokratikus országok számára. Természetesen mindez nem jelenti azt, hogy a regionális vagy nemzeti MI szabályozás ne tükrözhetne sajátos meglátásokat vagy irányzatokat, illetve ne lenne szükség arra, hogy ezen szabályozások, stratégiák a helyi kulturális, vallási, szociális és gazdasági szempontokat is figyelembe vegyék. Sőt, ennek épp az ellenkezője jelenthető ki, hiszen a helyi szabályozásnak és stratégiáknak – az adott nemzetközi vagy irányadó regionális, szövetségi keretrendszeren belül – a helyi közösségek értékeit, valamint a nemzeti gazdasági érdekeket is meg kell jelenítenie, illetve arányos módon képviselnie kell.

Ahogy az a fentiekből is látszik, mind nemzetközi, mind regionális vagy nemzeti szinten alapvetően multidiszciplináris szabályozási megközelítésre van szükség, amely számos szektor és gazdasági szereplő tekintetében az MI által jelentett kockázatokkal arányos, globális keretrendszerből kiinduló szabályozást tekint alkalmazandónak.[77] Napjainkban alapvetően mind nemzetközi, regionális vagy nemzeti szinten a különböző MI stratégiák, etikai iránymutatások és hasonló dokumentumok sokaságával szembesülhetnek, amelyek a fentiek szerint az adott közösségek, kormányzatok szempontjait tükrözik az MI-rendszerek megfelelő alkalmazásáról, valamint az innováció adott közegben való megfelelő támogatásáról. Ezek további, részletes áttekintésétől eltekintünk, a nemzeti stratégiák meghatározására példaként azonban fontosnak tartjuk röviden a magyar stratégia ismertetését.

Magyarország Mesterséges Intelligencia Stratégiája nem határoz meg külön alapelveket, és alapvetően a nemzetközi, valamint az európai szabályozási keretrendszerre támaszkodik, az ennek keretén belül lefektetett alapelvekből indul ki.[78] A dokumentum azonban konkrét célrendszert határoz meg, amely egyben azonosítja és fel is ismeri az MI társadalomra és gazdaságra gyakorolt hatásainak jelentőségét. Így a dokumentum a magyar MI stratégia célrendszerének keretében az alábbiakat határozza meg, illetve állapítja meg:

[77] Sonja ZILLNER, Jon Ander GOMEZ, Ana García ROBLES, Thomas HAHN, Laure Le BARS, Milan PETKOVIC, Edward CURRY: Data Economy 2.0: From Big Data Value to AI Value and a European Data Space. In: Edward CURRY, Andreas METZGER, Sonja ZILLNER, Jean-Christophe PAZZAGLIA, Ana García ROBLES (eds.): *The Elements of Big Data Value. Foundations of the Research and Innovation Ecosystem*. Cham, Springer, https://doi.org/10.1007/978-3-030-68176-0_16. 385.

[78] Magyarország Mesterséges Intelligencia Stratégiája 2020-2030, 2020. május, https://ai-hungary.com/api/v1/companies/15/files/137203/view

- az MI már a jelen technológiája,
- az MI átalakítja az emberek életét,
- az MI meghatározó lesz a gazdasági versenyképesség szempontjából,
- az MI alapvetően befolyásolja a társadalom egészét és határozza meg annak vezetését, szolgálatát,
- az MI globális technológia, amely újraértelmezi az együttműködési formákat és a nemzetközi viszonyokat,
- az MI pragmatikus technológia, valós hatásokkal.[79]

Mindemellett a dokumentum a magyar MI stratégia célrendszerét akként foglalja össze, miszerint „*Együtt tanuljuk, hatékonyan fejlesztjük és használjuk az MI technológiákat, felelősen, keretezetten, globális partnerként, a hétköznapok szolgálatában*”.[80] Mindezen megállapítás és elhatározás álláspontunk szerint is kétségtelenül reális és eredményes célkitűzést ad az MI-vel való felelős stratégiai tervezés számára.

A fentieken túl leszögezendő, hogy az MI rendszerek alkalmazása során az egyes alapvető jogok védelmét biztosító emberi jogi egyezmények rendelkezései is tiszteletben tartandók (különösen a személyes adatok kezeléséhez használt, vagy természetes személyekre jogaira, szabadságaira egyébként hatással bíró MI-rendszerek esetén), ideértve például az Emberi Jogok Európai Egyezményét, különösen annak 8. cikke szerinti magán- és családi élet tiszteletben tartásához fűződő jogot. Így például – az Emberi Jogok Európai Bíróságának („**EJEB**”) gyakorlata tükrében – a fenti jog sérelmével járhat a hatóságok általi titkos adatgyűjtés, amely az érintett régmúltbéli politikai, illetve erőszakszervezetben lévő tagságához kapcsolódik.[81] Az EJEB gyakorlata értelmében ugyanis a „magánélet” a 8. cikk kontextusában tágan értelmezendő, e körbe tartozhatnak akár az érintett üzleti, szakmai kapcsolatai is, így az érintett üzleti tevékenysége körében végzett kapcsolattartására vonatkozó titkos hatósági feljegyzések is az érintett magánélethez való jogának sérelmével járhatnak.[82] Mindez természetesen nem értelmezendő akként, hogy a jogszerűen végzett hatósági vagy titkosszolgálati adatkezelés feltétlenül a magánélet vagy a személyes adatok védelmének aránytalan sérelmével járna, illetve akként sem, hogy az érintettek múltbeli cselekményeit a hatóságok vagy a nagy

[79] Magyarország Mesterséges Intelligencia Stratégiája, 17-18.
[80] Magyarország Mesterséges Intelligencia Stratégiája, 18.
[81] Rotaru v. Romania, no. 28341/95., 2000. május 4-i ítélet, 43. bek.
[82] Amman v. Switzerland, no. 27798/95., 2000. február 16-i ítélet, 65–67. bekezdések

nyilvánosság adott esetben ne értékelhetnék megfelelően, azonban az érintettek magánéletéhez és személyes adatai védelméhez való joga kizárólag szükséges esetekben és arányos mértékben korlátozható, amely követelménynek az MI általi adatkezelés esetén is érvényesülnie kell. Mindez azért is fontos, mivel az emberi jogi követelményeket kiegészíthetik ugyan az MI-vel kapcsolatos nemzetközi iránymutatások, azonban ez utóbbiak nem szabad, hogy elvonják a figyelmet az előbbiekre, és értelemszerűen összetűzésbe sem kerülhetnek velük.[83]

b. A mesterséges intelligencia szabályozása az Európai Unióban

Az elmúlt időszakban szintén jelentős jogfejlődésnek lehettünk tanúi az európai MI szabályozása területén. Így az Európai Unió kiemelt figyelmet fordított az MI jelentette társadalmi és gazdasági hatásokra, valamint a technológia hatékony szabályozására. Az európai jogalkotó azonban az MI-rendszerek és különböző MI-modellek kapcsán elsődlegesen általános szabályozás bevezetése mellett döntött, amely átlátható keretet biztosítana az MI-rendszerek alkalmazására, valamint az egyes MI-modellek fejlesztésére az EU-n belül.

A fentiekre tekintettel 2018 áprilisában jelent meg a Bizottság Közleménye a Mesterséges Intelligenciáról Európának,[84] amely az MI helyzetével, a benne rejlő lehetőségekkel, valamint az Európai Unió piacára, technológiai fejlődésére gyakorolt hatásairól szól, továbbá ugyancsak felállításra került egy Magas-Szintű Szakértői Csoport az MI területén (angolul: „*High-Level Expert Group on Artificial Intelligence*"; „**Szakértői Csoport**"), amelynek feladata, hogy javaslatokat fogalmazzon meg az MI-vel kapcsolatos egyes közép-, illetve hosszútávú kihívások kezelése kapcsán, valamint hogy emellett a technológiával kapcsolatos etikai iránymutatásokat készítsen. A Csoporton kívül a Bizottság szintén létrehozta az Európai MI Hálózatot (angolul: „*European AI Alliance*"), valamint annak platformját, amelyek célja a témával kapcsolatos szakértői diskurzus, együttműködés megteremtése, biztosítása.[85]

[83] LANE (2022) op. cit. 927.
[84] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A közös európai adattér kialakítása felé, Brüsszel, 25.4.2018, COM(2018) 237 final
[85] European Commission, Commission appoints expert group on AI and launches the European AI Alliance, DIGIBYTE, European Commission, 2018.06.14, https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance

A fenti kezdeti lépéseket követően, 2018. decemberében jelent meg a Bizottság újabb közleménye, a mesterséges intelligenciáról szóló összehangolt tervről,[86] amely kiemelt területként tekint az oktatásra, valamint a megbízható MI technológiák megerősítésére és elterjesztésére. Nem sokkal később, 2019. áprilisában jelent meg a Bizottság „Az emberközpontú mesterséges intelligencia iránti bizalom növelése" elnevezésű közleménye,[87] amely a Szakértői Csoport ajánlásainak figyelembevételével hét olyan, alábbi követelményt állapít meg, amelynek a megbízható MI-alkalmazások meg kell, hogy feleljenek:

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

A fenti közlemény kiemeli továbbá, hogy bár ezen követelmények valamennyi MI megoldásra általánosságban alkalmazandók, az MI megoldások alkalmazásával kapcsolatos környezet sajátosságai is figyelembe veendők.[88]

A fenti dokumentumot követően 2020. februárjában jelent meg a „Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése",[89] 2021. áprilisában pedig a Bizottság „A mesterséges intelligenciával kapcsolatos európai megközelítés előmozdítása"[90] című közleménye, amelyek további meglátásokat tartalmaztak az MI európai megfelelésével és a vonatkozó európai jogalkotói elvárásokkal kapcsolatban. Szintén 2021. áprilisában jelent meg az európai jogalkotás szempontjából forradalminak számító mesterséges intelligenciáról szóló

[86] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A mesterséges intelligenciáról szóló összehangolt terv, Brüsszel, 2018.12.7., COM(2018) 795 végleges
[87] 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, Brüsszel, 2019.4.8., COM(2019) 168 final, 2.1.
[88] Uo.
[89] Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, Brüsszel, 2020.2.19. COM(2020) 65 final
[90] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A mesterséges intelligenciával kapcsolatos európai megközelítés előmozdítása, Brüsszel, 2021.4.21. COM(2021) 205 final

jogszabály („**MI Rendelet**”) tervezete,[91] amely a különböző MI-rendszerek kapcsán kockázatalapú megközelítést alkalmaz, és ennek megfelelően állít fel tilalmakat, illetve támaszt az MI-rendszerekkel, valamint szolgáltatóikkal és az azokat alkalmazó egyéb személyekkel, szervezetekkel szemben különböző követelményeket. A fenti tervezet áttekintését követően a Tanács 2022. decemberi olvasatában több szempontból felülvizsgálta, ideértve az MI-rendszerek meghatározását, az egyes rendszerek kategorizálását és a kapcsolódó követelményeket.[92] Ezt követően 2023. június 14-én jelent meg az Európai Parlament jelentése az MI Rendelet tervezetének felülvizsgálatáról,[93] amely a tervezet szövegét számos tekintetben tovább finomította, majd 2023. december 9-én az Európai Tanács elnöksége és az Európai Parlament tárgyalófelei átmeneti egyezségre jutottak, amely további módosításokhoz vezetett az MI Rendelet tervezete kapcsán, ideértve – többek között – a magas kockázatú MI-rendszerekre és általános célú MI-modellekre vonatkozó szabályokat, a tilalmazott MI-gyakorlatok körét és az az alóli kivételeket. Jelentős fejleménynek tekinthető továbbá az alapjogi hatásvizsgálat előírása a magas kockázatú MI-rendszerek alkalmazóival szemben, amely vélhetőleg tovább csökkenti az ilyen rendszerek alkalmazásával kapcsolatos kockázatokat.[94] Az általános célú MI-modellekkel kapcsolatos szabályok az MI Rendeletben különös jelentőséggel bírnak, tekintettel arra, hogy egyes modellek és azokra épülő rendszerek képességei, például a szövegelemzés, hang-, illetve videótartalmak generálása kapcsán, különösen jelentőssé váltak, kiemelt mennyiségű eredeti tartalmat állítva elő felhasználók által adott mintákból.[95] A véglegesnek szánt 2024. január 26-i dátumú szöveg végül 2024. február

[91] 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, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, Brüsszel, 2021.4.21, COM(2021) 206 final, 2021/0106(COD). Az értekezésben az MI Rendelet tervezet alábbi, helyesbített verziójára támaszkodtunk: Helyesbites az Európai Parlament által 2024. március 13-án a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet és a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló jogszabály) szóló (EU) 2024/... európai parlamenti és tanácsi rendelet elfogadására tekintettel első olvasatban elfogadott álláspontho, P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), cor01. 17.4.2024.

[92] European Council, Press release, Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights, 2022.12.06, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

[93] Európai Parlament, Jelentés a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról - A9-0188/2023, 2023.05.22, COM(2021)0206.

[94] Lásd: European Council, Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world, 2023.12.09, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

[95] Josh A. GOLDSTEIN, Girish SASTRY, Micah MUSSER, Renée DIRESTA, Matthew GENTZEL, Katerina SEDOVA: *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*, January 2023, arXiv:2301.04246. 15.

2-án került publikálásra, ezt követte a jogszabály-szöveg fenti hivatkozott 2024. április 17-i helyesbítése.

Az MI Rendelet kapcsán leszögezendő továbbá, hogy a jogszabály az MI-rendszerek, illetve az általános célú MI-modellek, nem pedig általánosságban az MI szabályozására hivatott. Ennek kapcsán az MI-rendszert akként határozza meg, mint olyan „*gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet*”.[96] Megemlítendő, hogy ezen meghatározás a nemzetközi dokumentumokban megjelenő MI-rendszer meghatározásra, így az OECD által elfogadott MI-rendszer meghatározására is alapoz.[97]

Hangsúlyozandó azonban, hogy az MI Rendelet az MI-rendszerek kapcsán sem valamennyi ilyen rendszert, illetve rendszer-használatot igyekszik szabályozni, így a jogszabálynak nem célja – a tagállamok szuverenitásának tiszteletben tartására tekintettel – az MI-rendszerek uniós jog hatályán kívül eső területeken, illetve nemzetbiztonsági célú alkalmazásának,[98] valamint a megfelelő eljárásrend keretein belül eljáró, harmadik országbeli hatóságok, nemzetközi szervezetek általi használat szabályozása sem,[99] ezekre értelemszerűen az irányadó nemzeti, illetve nemzetközi jogi követelményekkel, jogszabályi előírásokkal összhangban kerülhet sor. Ugyancsak nem tartoznak a jogszabály hatálya alá – többek között – a kizárólag tudományos kutatási és fejlesztési célból fejlesztett és üzembe helyezett MI-rendszerek és modellek, illetve azok kimenetei,[100] továbbá az MI-rendszerekkel vagy modellekkel kapcsolatos, azok forgalmazását vagy üzembe helyezését megelőző kutatási, tesztelési vagy fejlesztési tevékenység (ide nem értve a valós körülmények közötti tesztelést),[101] valamint az MI-rendszerek természetes személyek általi személyes, nem szakmai tevékenység során történő használata.[102] Így ez utóbbi felhasználás esetén hasonló szabályok érvényesülhetnek, mint

[96] MI Rendelet 3. cikk 1. pontja
[97] Az MI-rendszer OECD által elfogadott, felülvizsgált definíciójához lásd: OECD, Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, 5 March 2024, https://doi.org/10.1787/623da898-en
[98] MI Rendelet 2. cikk (3) bek.
[99] MI Rendelet 2. cikk (4) bek.
[100] MI Rendelet 2. cikk (6) bek.
[101] MI Rendelet 2. cikk (8) bek.
[102] MI Rendelet 2. cikk (10) bek.

például a személyes adatok magáncélú felhasználása kapcsán (ún. háztartási célú adatkezelés);[103] erre tekintettel a szabályozás hatókörén kívül eshetnek például a magán-, illetve hobbicélból, szabadidő töltése során történő felhasználási esetek (például: szórakozásképp családtagok, barátok arcképének kicserélése hírességekével „arccserélő" alkalmazáson keresztül).[104] Megemlítendő azonban, hogy az ezekkel kapcsolatos egyes magatartások (például: az ilyen felvételek nyilvánosságra hozatala) kapcsán egyéb jogszabályi rendelkezések irányadók lehetnek (például: személyes adatok védelméhez fűződő és egyéb személyiségi jogok, szerzői és szomszédos jogok védelme).

Az MI Rendelet szabályozásának címzettje elsősorban az MI-rendszer szolgáltatója. Az MI Rendelet értelmében a szolgáltató „*olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely MI-rendszert vagy általános célú MI-modellt fejleszt vagy fejlesztet, és a saját neve vagy védjegye alatt – akár fizetés ellenében, akár ingyenesen – az MI-rendszert vagy az általános célú MI-modellt forgalomba hozza, vagy az MI-rendszert üzembe helyezi*".[105] Ennek tükrében az MI Rendelet elsődlegesen az olyan személyekkel vagy szervezetekkel szemben állít fel követelményeket, amelyek az MI-rendszereket vagy általános célú MI-modelleket kifejlesztik vagy saját nevük alatt forgalomba hozzák, illetve üzembe helyezik. Emellett azonban az MI Rendelet az egyéb piaci szereplőkkel, illetve alkalmazókkal szemben is meghatároz bizonyos követelményeket, tekintettel arra, hogy ezek is végezhetnek ezen rendszerekkel vagy modellekkel kapcsolatban olyan tevékenységet, amelyek veszélyekkel, illetve kockázatokkal járhatnak az érintettek, vagy általánosságban a társadalom számára.

A fentebb említettek szerint az MI Rendelet kockázat-alapú megközelítést alkalmaz, így az egyes rendszerekkel kapcsolatos tilalmak, valamint követelmények az MI-rendszerek vagy MI-gyakorlatok egyfajta kategóriába sorolására építenek, akként, hogy a magasabb kategóriába tartozó rendszerekre vonatkozóan szigorúbb szabályok alkalmazandók, míg bizonyos MI-gyakorlatok teljesen, illetve szűk kivételektől eltekintve, tilalmazásra kerültek. Segítségképpen az MI Rendelet által meghatározott főbb kategóriákat az alábbi táblázatban foglaltuk össze néhány releváns példa megadása mellett.

[103] GDPR (18) preambulum-bekezdése
[104] Hangsúlyozzuk, hogy a tagállami jog a személyiségi jog védelme kapcsán támaszthat követelményeket azon esetekben is, ahol az MI Rendelet vagy a GDPR nem alkalmazandó.
[105] MI Rendelet 3. cikk 3. pontja

Kategória	Példák
Tiltott MI-gyakorlatok, illetve rendszerek[106]	Személyek egy meghatározott csoportjának tagjai sebezhetőségét kihasználó MI-rendszerek, illetve ezek alkalmazása[107]
Nagy kockázatú MI-rendszerek	Egyes toborzás céljára használt MI-rendszerek[108]
Alacsony kockázatú MI-rendszerek	Egyes generatív MI alkalmazások, ideértve például a chatbot alkalmazásokat[109]
Elenyésző kockázatú vagy kockázatot nem jelentő MI-rendszerek[110]	MI-alapú megoldást alkalmazó videójátékok

Hangsúlyozandó, hogy a fenti kategóriák az MI-rendszerekre irányadók, így az általános célú MI modellekre vonatkozó specifikus követelményeket az erről szóló külön fejezetben ismertetjük. Kiemelendő továbbá, hogy a fenti példák mellett is előfordulhatnak olyan megoldások vagy alkalmazási módok, amelyek egy-egy rendszer szigorúbb kategóriába sorolását teszik szükségessé. Így például, ha egy MI-alapú videójáték olyan szubliminális vagy egyéb technikákat alkalmaz, amely az azt használó gyermekeket ön- vagy közveszélyes magatartásra sarkallja, úgy adott esetben tiltott MI-gyakorlatnak is minősülhet, annak ellenére, hogy az MI-alapú megoldást alkalmazó videójátékok (amelynek napjainkban a videójátékok jelentős része tekinthető) a vonatkozó iránymutatások figyelembe vétele esetén jellemzően nem tekinthetők különösebben veszélyesnek az azt használó, ajánlott életkori kategóriába tartozó felhasználókra nézve. Mindez egyben azt is jelenti, hogy az MI Rendeletben meghatározottakon túl az egyes rendszerek szolgáltatóinak gondosan fel kell mérniük az adott rendszer alkalmazásával járó hatásokat, valamint figyelembe kell venniük a rendszer, illetve alkalmazása kapcsán irányadó egyéb jogszabályi követelményeket is (ideértve például: az egyes termékekre és rendszerekre vonatkozó, valamint az adatvédelmi, fogyasztóvédelmi és egyéb szektorális jogszabályi rendelkezéseket).

[106] Hangsúlyozandó, hogy az MI Rendelet 5. cikke a tiltott MI-gyakorlatok meghatározására épít, azonban értelemszerűen e körbe tartoznak a kizárólag e gyakorlatok megvalósítására létrehozott rendszerek is.
[107] MI Rendelet 5. cikk (1) bek. b) pontja
[108] MI Rendelet III. melléklet 4. a) pontja
[109] MI Rendelet 50. cikk (1) bek.
[110] Ezen kategóriát közvetlenül nem szabályozza az MI Rendelet, azonban a további kategóriákból értelemszerűen következik egy elenyésző vagy kockázatot nem jelentő kategória is.

A fentiekkel összhangban az MI Rendelet meghatározza azon MI-gyakorlatokat, amelyek a demokratikus társadalmak, valamint az érintettek alapvető jogainak védelme érdekében elfogadhatatlannak, és egyúttal tiltottnak minősülnek.[111] Így tiltottnak minősülnek az olyan MI-gyakorlatok, illetve az olyan MI-rendszerek forgalomba hozatala, üzembe helyezése vagy használata, amelyek

- szubliminális technikákat alkalmaznak az adott személy tudatán kívül, vagy célzottan manipulatív vagy megtévesztő technikákat alkalmaznak azzal a céllal vagy olyan hatás érdekében, hogy lényegesen torzítsák az adott személy vagy személyek egy csoportjának magatartását, jelentősen gyengítve megalapozott döntéshozatalra való képességüket, azt eredményezve, hogy olyan döntést hozzanak, amelyet egyébként nem hoztak volna meg, és amely ezen személyek részére jelentős károsodást okoz vagy ésszerű valószínűséggel okozhat,
- az adott személy vagy személyek egy meghatározott csoportjának sebezhetőségét használják ki azzal a céllal vagy hatással, hogy az adott személy vagy az adott csoporthoz tartozó személyek magatartását lényegesen torzítsák, és ennek révén jelentős károsodást okoznak vagy ésszerű valószínűséggel okozhatnak,
- természetes személyek vagy azok egy csoportjának egy adott időszakon belüli értékelésére vagy osztályozására használnak azok szociális viselkedése vagy egyéb jellemzői alapján, (i) hátrányos vagy kedvezőtlen bánásmódhoz vezetve az adatok létrehozásától vagy gyűjtésétől eltérő szociális kontextusban, illetve (ii) olyan hátrányos vagy kedvezőtlen bánásmódhoz vezetve, amely indokolatlan vagy aránytalan közösségi magatartásukhoz vagy annak súlyosságához képest,
- bizonyos kivételtől eltekintve olyan rendszerek, amelyek célja, hogy felmérjék vagy előre jelezzék annak kockázatát, hogy egy adott természetes személy bűncselekményt követ el,
- az internetről vagy kamerarendszerekből való, nem célzott lekérdezéssel arcfelismerő adatbázisokat létrehozó vagy bővítő rendszerek,
- a természetes személyek érzelmeiből következtetést levonó rendszerek munkahelyek vagy oktatási intézmények területén (ide nem értve orvosi vagy biztonsági okból üzembe helyezett, illetve forgalomba hozott rendszereket),

[111] MI Rendelet 5. cikk (1) bek.

- bizonyos kivételektől eltekintve olyan biometrikus kategorizálási rendszerek, amelyek természetes személyeket biometrikus adataik alapján egyénileg kategorizálnak bizonyos szenzitív tulajdonságok kikövetkeztetése céljából,
- bizonyos kivételektől eltekintve „valós idejű" távoli biometrikus azonosító rendszerek használata a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból.[112]

Az MI Rendelet indokolt esetekben, különösen egyes hatósági alkalmazások során a fenti tilalmak alól bizonyos kivételeket enged, ideértve például adott esetben a „valós idejű" távoli biometrikus azonosító rendszerek bizonyos esetekben való alkalmazását. Kétségtelen, hogy az ilyen megoldásokat egyre gyakrabban használják az érintettek azonosítására, a technológia pedig számos viselkedési minta alapján képes lehet személyek azonosítására, amely jelentős adatvédelmi kockázatokkal is bírhat,[113] ezért az ilyen megoldásokkal kapcsolatos tilalmak, illetve korlátozások észszerűnek tűnhetnek. Érdekes kérdésnek tekinthető a fentiek kapcsán azonban, hogy a fenti MI-gyakorlatok tilalma alól indokolt esetben engedhető-e további kivétel olyan esetekben is, ahol azt az MI Rendelet azt egyébként nem tenné lehetővé, azonban az adott esetben nagyobb hátrányok elkerülése érdekében indokolt lehetne (mintegy szükséghelyzetként). Amennyiben pedig erre a válasz igen, úgy kérdésként merül fel, hogy ennek kapcsán az adott MI-gyakorlat kivételes folytatásáról mely személy, illetve szervezet jogosult dönteni, illetve milyen feltételek figyelembevételével. Például egy bankrablás során dönthet-e úgy a rendőrség, hogy az elkövetővel vagy elkövetőkkel szemben olyan MI-rendszert alkalmaz, amely képes az elkövetők viselkedésének szubliminális technikák útján történő torzítására, vagy sebezhetőségének kihasználására, érzelmi befolyásolására (például: tusztárgyalás során, az elkövető hangjának, érzelmi állapotának, hátterének elemzésével). Ezen MI-alkalmazást ugyanis adott esetben indokolttá teheti a bankban és környékén tartózkodó, túszul ejtett személyzet és látogatók, valamint a rendőri személyzet biztonságának védelme, valamint az elkövető, illetve elkövetők elfogásához és felelősségre vonásához fűződő társadalmi érdek. Kérdéses azonban, hogy egy-egy ilyen eseti kivétel megengedése precedenst teremtene-e akár más kisebb súlyú, vagy a technológia alkalmazását kevésbé indokolttá tevő esetekben is. Megjegyzendő továbbá, hogy amennyiben a fenti alkalmazásra sor is kerülhet, annak természetesen kivételt kell képeznie, az irányadó tagállami és nemzetközi jogi követelményekkel összhangban kell érvényesülnie, valamint nem vezethet a technológia

[112] Uo.
[113] Omer TENE: Privacy: The new generations. *International Data Privacy Law*, vol. 1., issue 1. (2011) 21. [a továbbiakban: TENE (2011)]

széleskörű, indokolatlan alkalmazáshoz (például: kiterjedt távoli biometrikus azonosítás alkalmazása valamennyi körözés alatt álló elkövető azonosítása és kézre kerítése érdekében).

A fenti tiltott gyakorlatok meghatározásán túl az MI Rendelet következő kategóriaként az ún. nagy kockázatú MI-rendszereket határozza meg, amelyek alkalmazása már nem tiltott, az ezen rendszerek alkalmazásával járó kockázatok azonban jellemzően még mindig olyan mértékűnek tekintendők, amelyek szigorúbb követelmények alkalmazását teszik szükségessé az ilyen rendszerekkel, valamint – elsődlegesen – szolgáltatóikkal szemben. A nagy kockázatú MI-rendszerek kapcsán az MI Rendelet meghatározza azon területeket, illetve ennek kapcsán az olyan rendszereket és alkalmazási módokat is, amelyek az érintettekre, valamint a demokratikus társadalom működésére jelentős kockázatokkal járnak. Az MI Rendelet meghatározása szerint e körbe tartoznak a természetes személyek egyes biometrikus azonosításai érdekében, valamint kritikus infrastruktúrák irányítása és működtetése körében, továbbá oktatási és foglalkoztatási környezetben (például: egyetemi felvétel, munkahelyi megfigyelés és értékelés), az alapvető magán- és közszolgáltatásokhoz és ellátásokhoz való hozzáférés keretén belül, bűnüldözési célú, valamint a migrációs, menekültügyi, illetve határellenőrzési és az igazságszolgáltatási és demokratikus folyamatok területén alkalmazott egyes MI-rendszerek.[114] A nagy kockázatú MI-rendszerek körébe azonban jellemzően nem tartoznak bele az adott szakterületek tevékenységét pusztán kiegészítő rendszerek, ideértve például az igazságszolgáltatás adminisztratív tevékenységeit támogató rendszereket (például: bírósági határozatok anonimizálását segítő rendszerek).[115]

A fentiek körében hangsúlyozandó, hogy az MI-rendszerek bűnügyi, valamint idegenrendészeti területen történő alkalmazása körében az MI Rendelet azon területeket, illetve alkalmazási módokat határozza meg, amelyek az érintettek jogai és érdekei, valamint a demokratikus társadalom működése kapcsán alapvető jelentőséggel bírnak, így az MI-rendszerek ezen körben, illetve ezen célokból való alkalmazása kapcsán indokoltnak tekinthető a jelentősebb jogalkotói fellépés, illetve korlátozás, ideértve bűnügyi alkalmazás körében például az érintett áldozattá válása kockázatának értékelését, poligráfként történő alkalmazást, bizonyítékok megbízhatóságának értékelése kapcsán történő alkalmazást.[116] A migráció és a menekültügy

[114] MI Rendelet III. sz. melléklete
[115] MEZEI Kitti: *A mesterséges intelligencia jogi szabályozásának aktuális kérdései az Európai Unióban*. In Medias Res, 2023/01. https://doi.org/10.59851/imr.12.1.4. 62.
[116] MI Rendelet III. sz. melléklet, 6. pontja a)-c) pontjai

területén az MI Rendelet szintén meghatároz olyan megoldásokat, illetve alkalmazási módokat, amelyek az emberi jogok tekintetében kirívó sérelemmel járhatnak, ideértve például migrációval, a menekültüggyel vagy a határigazgatással összefüggésben történő egyes felhasználásokat.[117] Mindez azért is fontos, mivel az algoritmus általi hiba vagy téves mintakövetés ezen a területen könnyen diszkriminatív gyakorlatok kialakításához (például: bizonyos országokból, területekről származók vízum-kérelmeinek elutasítása), illetve történelmi igazságtalanságok bebetonozásához vezethet.[118]

A fentiek tükrében tehát elmondható, hogy a nagy kockázatú MI-rendszerek kapcsán az MI Rendelet elsődlegesen olyan MI-rendszerekre fókuszál, amelyek egy-egy területen való alkalmazása adott esetben kiemelt kockázatokkal járhat az érintettek jogaira és szabadságaira, valamint a demokratikus intézményrendszerek működésére nézve. Ezek tekintetében kiemelt figyelmet kaptak a különböző értékeléshez, valamint a biometrikus azonosításhoz használt, illetve a kritikus infrastruktúra üzemeltetésével, különböző alapvető szolgáltatások nyújtásával, illetve a bűnügyi és idegenrendészet területen, az igazságszolgáltatási területen, illetve demokratikus folyamatok kapcsán történő alkalmazásra szolgáló MI-rendszerek. Természetesen ennek kapcsán az MI Rendelet vonatkozó mellékletében felállított lista nem tekinthető kőbe vésettnek, hiszen a technológia fejlődésével, valamint a társadalmi és gazdasági folyamatok változásával egyes alkalmazási módokkal járó kockázatok csökkenhetnek, míg adott esetben bizonyos kockázatok növekedhetnek, új megoldások vagy alkalmazási módok jelenhetnek meg. Egyes rendszerek, alkalmazási módok vagy megoldások kapcsán továbbá olyan érvek is nagyobb hangsúlyt kaphatnak a közeljövőben, mint a közbiztonság vagy súlyos bűncselekmények, vagy egyéb, személy- és vagyonbiztonságot tömegesen veszélyeztető cselekmények megelőzése.

A pontozás és értékelés kapcsán is számos olyan érv merülhet fel, amelyek meghatározott esetekben, illetve szűkebb körben alátámaszthatják a technológia alkalmazásának szükségességét, különösen meghatározott pozíciókra történő kiválasztás során, annak emberi felülvizsgálat mellett történő alkalmazása esetén. Így egyes MI-rendszerek például az olyan jelentős felelősséggel járó munkakörökben történő kiválasztás során nyújthatnak segítséget,

[117] MI Rendelet III. sz. melléklet, 7. pontja
[118] Clarisse LAUPMAN, Laurianne-Marie SCHIPPERS, Marilia Papaléo GAGLIARDI: Biased Algorithms and the Discrimination upon Immigration Policy. In: Bart CUSTERS, Eduard FOSCH-VILLARONGA: *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*, The Hague, T.M.C. Asser Press, 2022. 200.

ahol a teljesítmény és az eredmények mérhetők (például: pilóták esetén repülési szimulációk során tanúsított pontosság). Álláspontunk szerint azonban ezen alkalmazások esetén is jellemzően szükségesnek mutatkozik az emberi felülvizsgálat, valamint az MI általi diszkrimináció elkerülésével kapcsolatos fokozott figyelem, amely kapcsán így csökkenthetők a hibás vagy diszkriminatív értékelésekből, döntésekből eredő kockázatok. Emellett álláspontunk szerint továbbá a teljeskörű vagy a társadalom nagyobb részét érintő pontozás önmagában is kiemelt társadalmi kockázatokkal járhat, például a hitelbírálati célú adatkezelések esetén.[119] Erre tekintettel a személyek nagyobb csoportjának, illetve ezen csoportok tagjai bizonyos jellemzőinek értékelésére szolgáló MI-rendszerek esetén különösen a tanítóadatkészlettel kapcsolatos reprezentativitás (például: a többségi mellett a sérülékeny csoportok jellemzőinek megfelelő megjelenítése), valamint a diszkriminatív minták kiszűrése jelenthet különösen kihívást.[120]

A nagy kockázatú MI-rendszerekre vonatkozó követelményeket az MI Rendelet III. fejezetének 2. szakasza határozza meg, ideértve az alábbiakat:

- kockázatkezelési rendszer,[121]
- adatokkal és adatkormányzással kapcsolatos követelmények,[122]
- műszaki dokumentáció elkészítése és naprakészen tartása,[123]
- naplózással és nyilvántartással kapcsolatos követelmények,[124]
- átláthatóság és az alkalmazók tájékoztatása,[125]
- emberi felügyelet biztosítása,[126]
- pontosság, stabilitás és kiberbiztonság.[127]

A fenti követelmények attól függetlenül irányadók az egyes nagy kockázatú MI-rendszerekre, hogy azokat személyes adatok kezelésére használják-e vagy sem. Tekintettel azonban ezen rendszerek általi adatkezelések jelentőségére, a fentiek kapcsán az MI-rendszerekhez kapcsolódó kockázatértékelési rendszerről, műszaki dokumentációról és a minőségi

[119] Ennek kapcsán lásd különösen az automatizált döntéshozatalról és a profilalkotásról szóló alfejezetben írtakat.
[120] ICO, How to use AI and personal data appropriately and lawfully, https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf, 4.
[121] MI Rendelet 9. cikk
[122] MI Rendelet 10. cikk
[123] MI Rendelet 11. cikk
[124] MI Rendelet 12. cikk
[125] MI Rendelet 13. cikk
[126] MI Rendelet 14. cikk
[127] MI Rendelet 15. cikk

kritériumoknak való megfelelésről, valamint az MI-rendszerekhez kapcsolódó naplózásról és nyilvántartásról, valamint tesztelésről az MI-ről és az adatbiztonságról szóló alfejezetben írunk bővebben.

A nagy kockázatú MI-rendszerek kapcsán kiemelt jelentőséggel bír továbbá az átláthatóság biztosítása, és az MI-rendszerek alkalmazóinak megfelelő tájékoztatása, tekintettel arra, hogy az ilyen rendszerek szolgáltatói és az azokat kínáló, illetve azokhoz hozzáférő egyéb piaci szereplők jellemzően információs előnyben vannak a rendszer által érintett felhasználókkal vagy egyéb személyekkel szemben, a rendszerek alkalmazói továbbá a szolgáltatók megfelelő tájékoztatása tükrében implementálhatják, illetve működtethetik megfelelően az adott rendszereket. Ennek keretében az ilyen MI-rendszereket olyan módon kell megtervezni és fejleszteni, hogy az alkalmazók a rendszer kimenetét értelmezni legyenek képesek, illetve azt megfelelően használhassák.[128] Az ilyen rendszerekhez továbbá digitális vagy egyéb formátumú használati utasítást kell mellékelni, ”*amely tömör, teljes körű, pontos és egyértelmű, az alkalmazók számára releváns, hozzáférhető és érthető információkat tartalmaz*”.[129] Az MI Rendeletben írt átláthatósággal kapcsolatos követelmények – ahogy a fentebb írt további követelmények is – az MI-rendszerekre attól függetlenül vonatkoznak, hogy azokat személyes adatok kezelésére használják-e, tekintettel azonban az MI jelentőségére a személyes adatok kezelése kapcsán, az MI-rendszerek átláthatóságáról bővebben az MI és az átláthatóság viszonyáról szóló alfejezetben írunk.

A nagy kockázatú MI-rendszerek kapcsán kiemelt jelentőséggel bír továbbá az emberi felügyelet biztosítása. Ennek kapcsán, többek között megfelelő ember-gép interfész eszközök révén, biztosítani szükséges, hogy a rendszert használatának időtartama alatt természetes személyek hatékonyan felügyelhessék.[130] Az emberi felügyeletet a rendszerbe beépített intézkedések, és/vagy egyéb megfelelő intézkedésekkel kell biztosítani, összhangban az MI-rendszer kockázataival, autonómia-szintjével és felhasználási kontextusával.[131] Megemlítendő azonban, hogy a gyakorlatban az emberi felügyelet későbbi lehetőségének tervezési és fejlesztési szakaszban történő biztosítása kihívásokba ütközhet a személyes adatok kezelését végző MI megoldások esetén, tekintettel arra, hogy – az adatvédelmi kockázatokon túl – számos

[128] MI Rendelet 13. cikk (1) bek.
[129] MI Rendelet 13. cikk (2) bek.
[130] MI Rendelet 14. cikk (1) bek.
[131] MI Rendelet 14. cikk (3) bek.

egyéb kockázat megelőzését is előre kell látniuk az adott MI rendszert tervező fejlesztő szakembereknek, ideértve különösen: az egészséget, biztonságot, alapvető jogokat fenyegető kockázatokat, amelyek kapcsán ezen szakemberek korlátozottabb képességekkel bírhatnak.[132] Mindemellett az MI Rendelet kiemeli továbbá, hogy „*nagy kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy megfelelő szintű pontosságot, stabilitást és kiberbiztonságot érjenek el*", amely követelményeket a rendszerek teljes életciklusa során következetesen teljesíteni kell.[133] A MI-rendszerek pontosságával kapcsolatos szempontok eltérőek lehetnek az adott rendszer típusa, alkalmazási területe, sajátosságai függvényében. Ez különösen azért lehet fontos, mivel a pontosság adatvédelmi alapelvi követelményként is megjelenik, ugyanakkor az MI alkalmazása eseten sokszor esetlegesen és nehezen meghatározható módon. A gyakorlatban például nagyobb fokú pontosság követelhető meg egy orvosi célra használt vagy egy vásárlói panaszokat feldolgozó alkalmazástól, mint egy irodalmi művek létrehozását vagy egy videójáték-fejlesztését támogató megoldástól.[134] Az adott MI-modell, illetve az azon alapuló rendszerek pontosabb működését egy ún. retrieval-augmented generation (RAG) keretrendszerre támaszkodás is segítheti, amely a modellt olyan külső forrásokhoz köti, amelyek felhasználása segíthet a pontosabb kimenetek létrehozásában, az MI általi „hallucinációk" (például: MI által kreált, kitalációkat megjelenítő válaszok) csökkentésében.[135]

A nagy kockázatú MI-rendszerek alkalmazása esetén az MI Rendelet a szolgáltatón túl az ellátási lánc egyéb szereplőire is követelményeket határoz meg, ideértve különösen az alkalmazót,[136] az importőrt[137] és a forgalmazót,[138] illetve ezen személyekre, és bármely más harmadik félre is a szolgáltatóra irányadó kötelezettségek alkalmazását rendeli, amennyiben e személyek vagy szervezetek

---

[132] Liane COLONNA: *Exploring the Relationship between Article 22 of the General Data Protection Regulation and Article 14 of the Proposed AI Act*. Faculty of Law, Stockholm University Research Paper No. 124, 2024.02.16, https://ssrn.com/abstract=4729206, http://dx.doi.org/10.2139/ssrn.4729206. 459-460.
[133] MI Rendelet 15. cikk (1) bek.
[134] ICO, Generative AI third call for evidence: accuracy of training data and model outputs, https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-third-call-for-evidence/
[135] IBM, What is retrieval-augmented generation?, https://research.ibm.com/blog/retrieval-augmented-generation-RAG
[136] MI Rendelet 3. cikk 4. pontja értelmében alkalmazó „*bármely olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely a felügyelete alá tartozó MI-rendszert használja, kivéve, ha az MI-rendszert személyes, nem szakmai jellegű tevékenység során használják*".
[137] MI Rendelet 3. cikk 6. pontja értelmében az importőr „*az Unióban tartózkodó vagy ott letelepedett természetes vagy jogi személy, aki vagy amely harmadik országban letelepedett természetes vagy jogi személy nevével vagy védjegyével ellátott MI-rendszert hoz forgalomba*".
[138] MI Rendelet 3. cikk 7. pontja értelmében a forgalmazó „*az a szolgáltatótól vagy importőrtől eltérő természetes vagy jogi személy az ellátási láncban, aki vagy amely az uniós piacon MI-rendszert forgalmaz*".

- saját nevükkel vagy védjegyükkel látják el a már forgalomba hozott vagy üzembe helyezett nagy kockázatú MI-rendszert (a felek közti eltérő szerződéses megállapodás hiányában);
- a már forgalomba hozott vagy üzembe helyezett nagy kockázatú MI-rendszeren jelentős módosítást hajtanak végre, akként, hogy az nagy kockázatú marad; vagy
- jelentősen módosítják az MI-rendszer, illetve általános célú MI-rendszer rendeltetését, amelyet nem minősítettek nagy kockázatúnak, és amelyet már forgalomba hoztak vagy üzembe helyeztek, akként, hogy az nagy kockázatú MI-rendszerré válik.[139]

A jogszabály kiemeli továbbá, hogy a fenti feltételek valamelyikének teljesülése esetén a rendszert eredetileg forgalomba hozó vagy üzembe helyező szolgáltató az MI Rendelet alatt a továbbiakban már nem tekinthető az MI-rendszer szolgáltatójának, és így rá az ezzel kapcsolatos követelmények sem vonatkoznak, a szolgáltató azonban – kivéve, ha az MI-rendszer nagy kockázatúvá alakítását előtte a vonatkozó megállapodásban vagy általános szerződési feltételeiben nem zárta ki – köteles együttműködni a helyébe lépő új szolgáltatóval, a számára a jogszabályi kötelezettségei teljesítéséhez szükséges, észszerűen elvárható technikai hozzáférést, dokumentációt megadni, egyéb kapcsolódó támogatást nyújtani (például: megfelelőségértékelés kapcsán).[140] A fenti rendelkezések különös jelentőséggel bírnak az egyes MI-rendszerek implementálása kapcsán. E körben a gyakorlatban különös jelentősége lesz a felek szerződéses megállapodásának és az abban lefektetett felelősségi, felhasználási szabályoknak, továbbá az adott rendszer esetleges implementáción túlmutató módosításainak, amelyek megváltoztathatják a felelősségi szerepeket.

Emellett az MI Rendelet további szabályokat határoz meg az egyes, speciális MI-rendszerekkel és modellekkel kapcsolatban, ideértve az általános célú MI-modelleket,[141] valamint az érintettekkel közvetlenül interakcióba lépő megoldásokat, az egyes generatív és deepfake megoldásokat létrehozó MI-rendszereket.[142] Erre tekintettel a közvetlenül természetes személyekkel interakcióba lépő rendszerek szolgáltatóinak – ide nem értve az egyes bűnügyi célú, megfelelő biztosítékok mellett alkalmazott MI-rendszerek szolgáltatóit – biztosítaniuk kell, hogy ezen rendszereket úgy tervezzék, hogy az érintettek tájékoztatást kapjanak arról,

[139] MI Rendelet 25. cikk (1) bek.
[140] MI Rendelet 25. cikk (2) bek.
[141] Az általános célú MI-rendszerekről és modellekről a dolgozat vonatkozó fejezetében írunk bővebben.
[142] MI Rendelet 50. cikke.

hogy MI-rendszerrel lépnek kapcsolatba, kivéve, ha ez a körülményekre és a felhasználási kontextusra figyelemmel, egy észszerűen jól tájékozott, figyelmes és körültekintő természetes személy szempontjából nyilvánvaló tény.[143] Az egyes, érzelemfelismerő és biometrikus rendszerek alkalmazóinak – a fentiek szerint az egyes bűnügyi célból alkalmazott rendszerek kivételével – szintén tájékoztatniuk kell az érintetteket az ilyen rendszerek alkalmazásáról.[144]

A fentiek mellett a deepfake tartalmakat létrehozó rendszerek szolgáltató, mind ezen tartalmak alkalmazói számára tájékoztatási kötelezettséget ír elő az MI Rendelet. Így a szintetikus tartalmakat létrehozó MI-rendszerek szolgáltatóinak – bizonyos kivételekkel – biztosítaniuk kell, hogy az MI-rendszer kimeneteit géppel olvasható formátumban jelöljék meg, és azok mesterségesen létrehozottként vagy manipuláltként észlelhetők legyenek.[145] Emellett alkalmazók esetén a képi, hang- és videótartalmak mesterséges létrehozásáról vagy manipulálásáról való tájékoztatást, illetve az egyes, jellemzően a véleménynyilvánítás szabadsága körébe eső tartalmak (például: egyes politikai mémek vagy egyéb szatirikus tartalmak, paródia-videók, művészeti alkotások) kapcsán a tartalmak megtekinthetőségével, élvezhetőségével összhangban álló, szűkebb körű figyelemfelhívást vár el; az MI Rendelet emellett a közérdekű ügyekről való tájékoztatása céljából közzétett szövegek generálása vagy manipulálása esetén is megköveteli a figyelemfelhívást, hacsak ezen tevékenység nem tartozik megfelelő szerkesztői ellenőrzés és felelősség alá.[146] A deepfake tartalmakat létrehozó MI-rendszerekről, az ilyen tartalmakról és azok adatvédelmi szempontjairól bővebben az értekezés vonatkozó fejezetében írunk.

Megemlítendő, hogy a fenti, interakciókkal, deepfake megoldásokkal kapcsolatos fenti tájékoztatást, illetve figyelemfelhívást egyértelmű és jól megkülönböztethető módon, legkésőbb az első interakció vagy kitettség alkalmával szükséges nyújtani az érintettek számára, szükséges esetén összhangban a vonatkozó akadálymentesítési követelményekkel.[147]

A fentiek mellett az MI Rendelet létrehozza az MI-hivatalt, amely a jogszabály érvényesítése kapcsán, valamint szakértelme révén segíti a Bizottságot és a jogalkalmazókat. Az MI-hivatal

[143] MI Rendelet 50. cikk (1) bek.
[144] MI Rendelet 50. cikk (3) bek.
[145] MI Rendelet 50. cikk (2) bek.
[146] MI Rendelet 50. cikk (4) bek.
[147] MI Rendelet 50. cikk (5) bek.

munkáját a tagállamok is támogatják.[148] Emellett az MI Rendelet az innovációt segítő intézkedéseket is meghatároz, így rendelkezéseket tartalmaz az ún. szabályozói tesztkörnyezetekre (angolul: „regulatory sandbox"), valamint az MI-rendszerek valós körülmények közötti tesztelésére, statup-ok támogatására.[149] A szabályozói tesztkörnyezetekre példaként említhető – az adatvédelmi gyakorlatból – a norvég adatvédelmi hatóság generatív MI alkalmazásokkal kapcsolatos homokozója, amelybe például a közegészségügyi ellátásokat vagy alternatív jogi szolgáltatásokat igénybe vevők támogatását célzó projektek kerültek befogadásra.[150] Vélhetően hasonló szabályozói tesztkörnyezeteknek, programoknak lehetünk majd a tanúi az MI Rendelet alkalmazásával is.

Hangsúlyozandó továbbá, hogy az MI Rendelet jelentős súlyú szankciókat vezet be az MI Rendeletben foglalt követelményeknek való meg nem felelés esetén, ideértve különösen a meg nem feleléssel kapcsolatos bírságtételeket. Így a tiltott MI-technikák alkalmazása esetén akár 35.000.000 euró, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 7 %-át kitevő összegű közigazgatási bírsággal is sújtható a jogsértő,[151] míg a legtöbb esetben a meg nem felelést az MI Rendelet – gazdasági szereplők vagy bejelentett szervezetek esetén – legfeljebb 15 000 000 EUR összegű, vagy ha az elkövető vállalkozás, az előző pénzügyi év teljes globális éves árbevételének legfeljebb 3 %-át kitevő összegű közigazgatási bírsággal sújtja.[152] Kérdéses azonban, hogy a gyakorlatban mely hatóság milyen esetekre milyen szankciókat alkalmaz majd. A GDPR tapasztalatai alapján ugyanis jelentősen eltérő bírságolási gyakorlat alakulhat ki az egyes tagállamokban, amely a vállalatokat is orientálhatja a joghatóság lehetséges körű megválasztásában.[153]

A fentiekre tekintettel a bírósági és hatósági jogértelmezés vélhetőleg különös jelentőséggel fog majd bírni a közeljövőben, az egyes MI-rendszerekkel, modellekkel kapcsolatos elvárások adatvédelmi szempontjainak, valamint az MI Rendelet és az adatvédelmi jogszabályok követelményeinek és gyakorlatának együttes értelmezése kapcsán. Mindez azért is fontos, mivel az adatvédelmi jogszabályok jelentős része, így a GDPR is technológiasemleges

[148] MI Rendelet 64. cikk (1)-(2) bekezdései
[149] MI Rendelet V. címe
[150] Datatilsynet, Time for generative AI in the sandbox, https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/time-for-generative-ai-in-the-sandbox/
[151] MI Rendelet 99. cikk (3) bek.
[152] MI Rendelet 99. cikk (4) bek.
[153] SZEGEDI László, DORNFELD László, POLGÁR Zoltán, Teleki Bálint: A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – egységes szabályozás, eltérő alkalmazás?. *Infokommunikáció és jog*, 2021/1. 15.

megközelítést alkalmaz, ez pedig a személyes adatok új technológiák révén végzett kezelése kapcsán is érvényesül,[154] ideértve az MI által végzett adatkezeléseket is, így jelenleg számos általános, a korábbi évtizedekben kimunkált adatvédelmi szabály és követelmény alkalmazandó új, rapid módon fejlődő technológiai környezetben.

A fentiek kapcsán kiemelendő azonban, hogy az MI Rendelet tervezetének korábbi szövegét adatvédelmi szempontból is kritikák érték az elmúlt időszakban, amely jellemzően a jogszabály-tervezet világosságával, valamint annak termékbiztonsági szempontú megközelítése és a GDPR követelményei közti különbségekkel, illetve az európai adatvédelmi gyakorlat elvárásainak figyelmen kívül hagyásával volt kapcsolatos. Ennek egyik okát képezte az MI Rendelet és a GDPR megközelítése közti alapvető különbség. Míg az MI Rendelet az egyes MI-rendszerekkel, illetve modellekkel kapcsolatos kockázatalapú szabályokat rögzít, a GDPR, illetve jellemzően az adatvédelmi jogszabályok jog-alapú megközelítést alkalmaznak, és az érintettek jogai mentén bontják ki a személyes adatok kezelőire vonatkozó követelményeket.[155] A tervezettel kapcsolatos, adatvédelmi szempontból a leginkább relevánsnak tekinthető aggályokat, kritikákat és javaslatokat az Európai Adatvédelmi Testület („**EDPB**”) és az európai adatvédelmi biztos vonatkozó közös véleménye foglalta össze.[156] E körben az 5/2021. Közös Vélemény kifejezetten felrótta a jogszabály-tervezet azon megközelítését, amellyel egyes csoportok vagy a társadalom egészére jelentett számos kockázatot figyelmen kívül hagyja (ideértve például a demokratikus társadalom működését veszélyeztető lehetséges hatásokat),[157] továbbá az MI Rendelet kockázatalapú megközelítése kapcsán a jogszabály-tervezet releváns szövegezésének a GDPR-al való összhangját hiányolta.[158] A fentieken túl az 5/2021. Közös Vélemény többek között szintén hiányosságként rótta fel, hogy a nagy kockázatú MI-rendszerek MI Rendelet III. mellékletében meghatározott listája több olyan megoldást sem tartalmaz, amelyek az érintettekre nézve jelentős kockázattal járhatnak (például: egyes egészségügyi kutatások kapcsán alkalmazott rendszerek).[159]

---

[154] PÉTERFALVI Attila: Algoritmusok és adatvédelem: Quo vadis? A 2020.02.27-i mesterséges intelligencia alkalmazásának hatása az alapjogokra című konferencián elhangzott előadás szerkesztett leirata. In: TÖRÖK Bernát, ZŐDI Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről*. Budapest, Ludovika Egyetemi Kiadó, 2021. 181.

[155] Josephine WOLFF, William LEHR, Christopher S. YOO: Lessons from GDPR for AI Policymaking. Virginia Journal of Law & Technology, vol. 27. no. 4. (2024) 20.

[156] Az EDPB 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 rendeletre irányuló javaslatról. 2021.06.18. („**5/2021. Közös Vélemény**”)

[157] 5/2021. Közös Vélemény 17. pontja

[158] 5/2021. Közös Vélemény 18. pontja

[159] 5/2021. Közös Vélemény 19. pontja

Az 5/2021. Közös Vélemény kiemelte továbbá több, az MI Rendelet tervezete által nagy kockázatúnak minősített rendszer tilalmának szükségességét, ideértve különösen az egyes bűnügyi célú megfigyeléssel kapcsolatos felhasználásokat. Ennek kapcsán a 5/2021. Közös Vélemény hangsúlyozta, miszerint „*MI rendőrségi és bűnüldözési célú használatához területspecifikus, pontos, előreláthatő és arányos szabályokra van szükség, amelyeknek figyelembe kell venniük az érintett személyek érdekeit és a demokratikus társadalom működésére gyakorolt hatásokat*”;[160] erre tekintettel az MI Rendelet vonatkozó szabályai jelentős mértékben módosultak, szűkítve, illetve konkretizálva azon estek körét, ahol az MI-rendszerek bizonyos bűnüldözési célokból, illetve hatóságok általi megfigyelés céljára alkalmazhatók.

Az 5/2021. Közös Vélemény ugyancsak szót emelt, és általános tilalmat követelt a közösségi pontozás kapcsán,[161] továbbá szorgalmazta, miszerint „*általános jelleggel tiltsák meg az MI-nek az emberi jellemzők – például az arc, a járás, az ujjlenyomat, a DNS, a hang, a billentyűleütések és más biometrikus vagy viselkedési jellemzők – alapján a nyilvánosság számára hozzáférhető helyeken történő automatikus felismerésre bármilyen összefüggésben történő használatát*”.[162] Emellett a dokumentum ugyancsak az MI általi érzelemfelismerés általános tilalma mellett foglalt állást, amely tekintetében csak szűk körű kivételeket tartott megengedhetőnek (ideértve az egészségügyi vagy a kutatási célú felhasználást).[163] Ezen észrevételek a jogszabály tervezetének felülvizsgálata során részben figyelembevételre is kerültek az általunk fentebb írtak szerint. Az érzelemfelismerés kapcsán továbbá megemlítendő, hogy ennek kapcsán az adatvédelmi hatósági gyakorlat is szigorú fellépést mutatott, így 2022-ben például Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság („**NAIH**”) egy magyarországi székhelyű bankkal szemben szabott ki 250.000.000,-Ft. összegű adatvédelmi bírságot hangfelétel, illetve érzelem-elemzéssel kapcsolatos adatkezelés kapcsán. A bank ugyanis az eset során az ügyfélszolgálati hívásokat érzelemfelismerő megoldással elemezte, és ennek kapcsán hozott döntést az ügyfélkapcsolataiban, valamint értékelte az ügyfélszolgálati munkatársak teljesítményét, az

[160] 5/2021. Közös Vélemény 27. pontja
[161] 5/2021. Közös Vélemény 29. pontja
[162] 5/2021. Közös Vélemény 32. pontja
[163] 5/2021. Közös Vélemény 35. pontja

érintettek számára jellemzően átláthatatlan módon, az érdekmérlegelés nem megfelelő módon történő elvégzése alapján.[164]

Az 5/2021. Közös Vélemény kiemelte továbbá a magas kockázatú MI-rendszerek esetén az általában harmadik fél által végzendő előzetes megfelelősértékelés fontosságát,[165] hangsúlyozta továbbá, hogy a szabályozásnak a már használatban lévő MI-rendszerekre is ki kell terjednie.[166] Emellett a dokumentum további meglátásokat tett az MI-rendszerek fejlesztésének és alkalmazásának adatvédelmi szempontjai kapcsán, ideértve a tesztkörnyezetet[167] és az átláthatóságot.[168] A fentiekkel összhangban hangsúlyozandó, hogy a fenti 5/2021. Közös Vélemény számos pontja figyelembevételre került az MI Rendelet szövegének véglegesítése kapcsán (például: a távoli biometrikus azonosítás tekintetében), azonban az MI Rendelet véglegesnek tekintett szövege számos, adatvédelmi szempontból kockázatosnak tekinthető megoldással szemben kizárólag részleges, bizonyos gyakorlatok tekintetében érvényesülő tilalmat állított fel, illetve enyhébbnek tekinthető követelményeket támasztott, ideértve például az érzelemfelismerést és egyes biometrikus azonosítási célú, valamint pontozással kapcsolatos MI-rendszereket és deepfake megoldásokat.

A Bizottság az MI Rendeletnek való megfelelés elősegítése, valamint a technológiai szektor szereplői együttműködésének és erőteljesebb szerepvállalásának támogatása érdekében meghirdette az MI Megállapodást (angolul: „*AI Pact*”), amelynek kapcsán a résztvevő vállalkozásokat 2024. első felében tervezi összehívni. Ennek keretében az érdeklődő, résztvevő vállalkozások önkéntesen, „eskü” (angolul: „*pledge*”) formájában még az MI Rendelet hatályba lépése, illetve kötelező alkalmazása előtt vállalhatják az MI Rendelet követelményeinek való megfelelést, továbbá hozzájárulhatnak az MI Rendelet értelmezésének, gyakorlati alkalmazásának elősegítéséhez, így az iparági megfelelési gyakorlatokat is aktívan formálhatják.[169] Mindez az MI Rendelet elfogadását és hatályba lépését követően remélhetőleg az EU-n belüli egységes jogértelmezés és jó gyakorlatok kialakítására serkentő hatással lesz.

[164] NAIH-85-3/2022. 86-87.
[165] 5/2021. Közös Vélemény 37. pontja
[166] 5/2021. Közös Vélemény 38-41. pontja
[167] 5/2021. Közös Vélemény 61-68. pontja
[168] 5/2021. Közös Vélemény 69-72. pontja
[169] European Commission, AI Pact, https://digital-strategy.ec.europa.eu/en/policies/ai-pact

A fentiek kapcsán meglátásaink szerint az MI Rendelet és az ennek kapcsán kibontakozó európai MI szabályozás általánosságban nem hátráltatja az MI-rendszerek fejlesztését, valamint az ilyen megoldások elterjedését, a kockázatalapú megközelítése révén pedig jellemzően a társadalmi szempontból kiemelt kockázatokkal bíró, nagy kockázatú MI-rendszerekre, valamint az általános célú MI-modellekre igyekszik fókuszálni. Világosnak tűnik továbbá, hogy az MI-rendszerek (különösen ideértve a nagy kockázatú MI-rendszereket és különösen veszélyes, tiltott MI-gyakorlatokat) vonatkozásában szükséges egy átlátható, egységes európai szabályozás kialakítása, amely egyértelmű követelményeket támaszt az MI-rendszerek európai piacokon való szolgáltatásával, alkalmazásával kapcsolatban. Ugyanakkor meglátásaink szerint a szabályozás túlzottan enyhe képet mutat bizonyos esetekben. Így például a deepfake tartalmak kapcsán jellemzően a puszta tájékoztatáson, figyelemfelhíváson túl további követelményt nem támaszt, holott érdemes lett volna e körben külön, tiltott vagy szigorúbban szabályozott kategóriát képezni az érintettek és a társadalom számára káros és veszélyes tartalmak vonatkozásában (például: bűncselekményt megvalósító, választási manipuláció céljából készített, illetve felhasznált tartalmak). Ugyancsak javasolt lett volna az alapjogi hatásvizsgálat elkészítésének eseteit a hatósági, illetve közszférán belüli alkalmazáson túl egyes üzleti célú alkalmazásokra is kiterjeszteni (például, ha azok az érintettek, különösen sérülékeny csoportokba tartozó személyek jelentős befolyásolására lehetnek hatással). Az ilyen MI-alkalmazások ugyanis adott esetben még az adatok anonimizálását követően is sérelmesek lehetnek az érintettekre nézve (bár kétségtelen, hogy az anonimizált adatok kezelése e körben jelentős lehetőségeket rejt magában, illetve jellemzően nagyobb védelmet nyújt az érintettek számára, mint a személyes adatok anonimizálás nélküli további kezelése).[170]

A fentieken túl természetesen az európai MI szabályozás jövőjével, és annak adatvédelmi, valamint egyéb szabályozásokkal való összhangjával kapcsolatban további kihívásokkal is számolhatunk, különös tekintettel a technológia egyre gyorsuló ütemű fejlődésére, valamint annak társadalmi és gazdasági hatásaira. A változó világ szabályai között azonban az európai MI szabályozás sok szempontból így is útmutatónak tűnik, és vélhetőleg mintaként szolgál majd az EU-n kívüli országok szabályozásai számára is a közeljövőben.

[170] Michèle FINCK, Frank PALLAS: They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, vol. 10., issue 1. (2020) 36.

c. A mesterséges intelligencia szabályozása az Amerikai Egyesült Államokban

Az utóbbi években az adatvédelem és a digitalizáció egyéb területei mellett jelentős lendületet kapott az amerikai MI szabályozás is, amelynek tekintetében fordulópontot jelentett a Donald Trump elnök által aláírt, 2019. februárjában megjelent 13859. sz. elnöki rendelet, [171] amely már első szakaszában meghirdeti az MI fejlesztéssel és alkalmazással kapcsolatos kormányzati stratégiát, az American AI Initiative-et, valamint annak alábbi öt alapelvét, illetve alapvető rendelkezéseit, célkitűzéseit:

- a technológiai kutatásban és fejlődésben való élenjárást,
- a megfelelő technikai követelményrendszer kialakítását, illetve a különböző akadályok lebontását,
- a megfelelő munkaerő képzését (ideértve a jelenlegi és az eljövendő generációkat is),
- a technológiával és annak megfelelő alkalmazásával kapcsolatos közbizalom kialakítását,
- a megfelelő nemzetközi környezet kialakítását, amely támogató az amerikai MI kutatással és fejlesztéssel, valamint ehhez piacokat nyit.

További jelentős lépést jelentett az amerikai MI szabályozás alapelveit meghatározó és egyben a közeljövő MI szabályozása számára szabályozási keretrendszert is biztosító, 2022-ben megjelent „*Blueprint for an AI Bill of Rights*" elnevezésű dokumentum („**Blueprint**"). Az amerikai MI szabályozás alapelvei közé ennek tükrében az alábbiak tartoznak:

- biztonságos és hatékony rendszerek,
- algoritmikus diszkrimináció elleni védelem,
- adatvédelem,
- figyelemfelhívás és magyarázat,
- emberi alternatívák, megfontolás és megoldás.[172]

A fentiekre tekintettel a dokumentum hangsúlyozza a megbízhatatlan és nem hatékony rendszerekkel szembeni védelmet, e körbe értve a nem megfelelő vagy nem releváns adatok

[171] Executive Order 13859 of February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence
[172] Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf. 5-7.

felhasználással szembeni védelmet is.[173] A dokumentum következő alapelvét képezi az MI általi, algoritmikus diszkriminációval szembeni védelem. Ennek kapcsán a dokumentum különösen kiemeli az algoritmusok és rendszerek méltányos használatát és tervezését, valamint az ezzel kapcsolatos kockázatértékelés fontosságát már a tervezési szakaszban.[174] A dokumentum kiemeli továbbá az amerikaiak jogait a visszaélésszerű adatkezelési gyakorlatoktól való védelemre beépített védelmi lehetőségek által, valamint hangsúlyozza az érintettek jogát az adataik felhasználásával kapcsolatos rendelkezésről.[175] Mindemellett hangsúlyozza továbbá az érintettek azon jogát, hogy tudomással bírjanak arról, hogy esetükben egy automatizált rendszer kerül alkalmazásra, valamint hogy megértsék, ez hogyan és miért vezet olyan döntésekhez, illetve eredményekhez, amelyek rájuk hatással bírnak. E körben kiemelten fontosnak tekinthető a közérthető nyelven történő fogalmazás a rendszer működésének egyértelmű összefoglalásával, az automatizáltság ismertetésével, valamint a rendszerért felelős megnevezésével és az eredmények megmagyarázásával.[176] Végezetül a dokumentum kiemeli az érintettek azon jogát, hogy amennyiben ez releváns és lehetséges, tiltakozhassanak az adatkezelés ellen, valamint, hogy elérhessenek olyan személyt, aki gyorsan képes áttekinteni és megoldani az érintett problémáját.[177] A fentiek szerint a dokumentum több esetben is a GDPR által írtak szerint, illetve ahhoz hasonlóan fogalmaz, ideértve például az érintettek tájékoztatását az automatizált rendszerekről, valamint adataik kezeléséről, és az érintettek ezzel kapcsolatos jogait. Azonban ezen túl egyéb szempontokat is kiemel, ideértve különösen az MI általi diszkrimináció megelőzésének fontosságát, valamint a kapcsolódó hatásvizsgálati kötelezettséget.

A fentiek mellett szintén jelentős lépésnek tekinthető az Egyesült Államok elnökének „*Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*” elnevezésű rendelete.[178] A rendelet elvárja a biztonsági tesztek kormányzattal való megosztását a legerősebb MI-rendszerek fejlesztőitől, továbbá sztenderdek, eszközök és tesztek előírását határozza meg az MI-rendszerek biztonságával és megbízhatóságával kapcsolatban, amellyel különösen a Nemzeti Szabványügyi és Technológiai Intézetet (angolul: „*National Institute of*

[173] Blueprint for an AI Bill of Rights, 5.
[174] Uo.
[175] Blueprint for an AI Bill of Rights, 6.
[176] Uo.
[177] Blueprint for an AI Bill of Rights, 7.
[178] The White House. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 2023.10.30, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

Standards and Technology", röviden: „**NIST**"), bízza meg valamint az egyes szakterületeken, illetve szempontok kapcsán egyéb kormányzati ügynökségeket is felhatalmaz (ideértve például a Kereskedelmi Minisztérium számára az egyes MI tartalmak észlelésével és csalások megelőzésével kapcsolatos iránymutatások elkészítésének előírását). A rendelet továbbá jelentős figyelmet szentel a személyes adatok védelmének, így elrendeli különösen a személyes adatok védelmével kapcsolatos technológiák fejlesztésének támogatását, valamint a személyes adatok ügynökségek általi gyűjtésének és felhasználásának értékelését. A fentieken túl a rendelet az érintetteket segítő technológiák fejlesztését támogató, illetve az érintettek védelmét célzó rendelkezéseket tartalmaz továbbá – többek között – olyan fontos területeken, mint a diszkrimináció-tilalom, a fogyasztók, a betegek és a diákok, valamint a munkavállalók védelme.

Ugyancsak jelentős fejleményt jelent az „Algorithmic Accountability Act"[179] elnevezésű törvény-tervezet, amelyet 2022. első felében nyújtottak be az amerikai törvényhozásban. A jogszabály-tervezet elsődlegesen az MI általi, algoritmikus diszkrimináció ellen kíván fellépni, valamint az egyes MI megoldások alkalmazásával kapcsolatos elszámoltathatóságot is hangsúlyosabbá tenné. E körben leszögezendő, hogy a törvény-tervezet kizárólag jelentős árbevétellel rendelkező, illetve jelentős számú érintettre hatással levő automatizált döntéshozatalt, illetve hasonló eljárásokat alkalmazó szolgáltatókra vonatkozna.[180] A törvény-tervezet szintén meghatározza azon területeket, ahol a döntéshozatal kritikusnak tekinthető, illetve társadalmi szempontból kiemelkedő jelentőséggel bír (ideértve például az oktatás, a foglalkoztatás, a pénzügyi szolgáltatás, az egészségügy vagy a lakhatás területét),[181] figyelembe véve, hogy ezen területeken a diszkrimináció kockázata jellemzően magasnak mondható.

A törvény-tervezet egyben meghatározza a fenti megoldások, eljárások alkalmazóival szembeni alapvető követelményeket, valamint előírja hatásvizsgálat elvégzését és dokumentálását, továbbá az ennek során figyelembe veendő, illetve értékelendő szempontokat és körülményeket is.[182] E körben kiemelt jelentőséggel bír az érintetti jogok figyelembevétele, amelynek kapcsán az adott, automatizált megoldást, illetve eljárást alkalmazó szervezetnek tájékoztatniuk kell az érintetteket ezen megoldás, illetve eljárás alkalmazásáról, valamint biztosítaniuk kell számukra

[179] Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/6580/text
[180] Algorithmic Accountability Act, sec. 2(7)
[181] Algorithmic Accountability Act, sec. 2(8)
[182] Algorithmic Accountability Act, sec. 3-4

az ezzel szembeni tiltakozáshoz való jogot is.[183] Mindemellett a fenti szervezeteknek szükséges azonosítaniuk az érintettekre vonatkozó valószínű negatív következményeket, illetve felmérniük és meghatározniuk az ezen következmények, károk csökkentése érdekében alkalmazandó releváns megközelítést, illetve stratégiát, e körbe értve

- a fenti valószínű negatív következmények, károk meghatározását, felmérését,
- a fentiek megelőzése vagy lehetséges körű csökkentése érdekében teendő lépéseket,
- azon negatív hatások azonosítását, amelyek elkerülése vagy enyhítése érdekében nem került sor intézkedések megtételére, illetve a vonatkozó érvek, érdekek meghatározását,
- a fentiek érdekében alkalmazott eljárásokat, gyakorlatokat, valamint annak meghatározását, hogy az adott szervezet alkalmazottjai megfelelő képzésben részesültek a fentiek kapcsán.[184]

Az algoritmusok általi diszkrimináció kockázataira tekintettel a fentieken túl az Egyesült Államok több kormányzati szerve (ideértve többek között a Szövetségi Kereskedelmi Bizottság ("*Federal Trade Commission*"; röviden: „**FTC**"), valamint az Igazságügyi Minisztérium állampolgári jogokkal foglalkozó osztályát) is közös nyilatkozatot bocsátott ki, amely az automatizált rendszerek általi diszkriminációval, előítéletekkel szembeni veszélyekre hívja fel a figyelmet, ideértve például a felhasznált adatokból, adatkészletekből, nem megfelelő társadalmi minták alapulvételéből származó visszaélések lehetőségét, az alkalmazott modellek átláthatóságával, valamint a nem megfelelő tervezésből és felhasználásból származó kockázatokat.[185]

A fentieken túl 2023-ban benyújtásra került az „Artificial Intelligence Research, Innovation, and Accountability Act" elnevezésű törvény-tervezet („**AIRIA**"),[186] amely az MI tudományos célra való felhasználását igyekszik támogatni, a fejlesztéssel kapcsolatos esetleges negatív hatások csökkentésével. Az AIRIA – európai mintára – alapvetően az ún. jelentős hatással bíró MI-rendszerekre („*high-impact artificial intelligence system*"), valamint az ún. kritikus MI-rendszerekre („*critical artificial intelligence system"*) terjed ki. A jelentős hatással bíró MI-

[183] Algorithmic Accountability Act, sec. 4(8)(A)
[184] Algorithmic Accountability Act, sec. 4(9)
[185] Federal Trade Commission, Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf
[186] Artificial Intelligence Research, Innovation, and Accountability Act of 2023, https://www.thune.senate.gov/public/_cache/files/7dea8daa-f6d1-4881-ad21-2381fcbe0785/6362CE1D0A17743166BC170A593B5CDA.ccaskfall23a15.pdf

rendszerek körébe tartoznak egyes, a társadalom számára különösen jelentős területeken (például: foglalkoztatás, egészségügy, biztosítás) joghatással vagy hasonló jelentős hatással bíró döntések meghozatalára szolgáló rendszerek,[187] míg az AIRIA a kritikus MI-rendszerek körébe egyes, a társadalom számára különösen jelentős hatásokkal bíró, például egyes kormányzati szervek által alkalmazott vagy a büntető igazságszolgáltatás területén használt MI-rendszereket sorol.[188] Az AIRIA továbbá azon, Egyesült Államok területén élő fogyasztók számára elérhető internetes platformokra (ideértve például: nyilvánosan elérhető weboldalak vagy applikációk, közösségi médiaoldalak, videómegosztó-platformok, keresőszolgáltatások) terjed ki, amelyek szolgáltatója a) az elmúlt 180 napon belül legalább 500 főt foglalkoztatott, b) az elmúlt 3 évben átlagosan legalább 50.000.000 dollár bruttó árbevétele volt, c) éves átlagban legalább 1.000.000 érintett adatait gyűjti össze vagy dolgozza fel, és d) nem kizárólag non-profit kutatási célból működik,[189] így a törvény-tervezet a legnagyobb szervezetek által alkalmazott legjelentősebb MI-rendszereket igyekszik szabályozás alá vonni. Ennek kapcsán a törvény-tervezet előírja például kritikus MI-rendszerek esetén megfelelő kockázatértékelés elvégzését,[190] valamint ilyen rendszerek tanúsítását,[191] továbbá átláthatósági jelentések tételét a jelentős hatással bíró MI-rendszerek szolgáltatói számára.[192] A törvény-tervezet továbbá a hatálya eső platformok kapcsán alkalmazott generatív MI-rendszerek kapcsán is előírja a felhasználók megfelelő tájékoztatását,[193] hasonlóan az MI Rendelet megközelítéséhez.

Az MI-rendszerek általi adatkezelés emellett a fentieken túl adott esetben személyiségi jogsértéssel is járhat, így például egy adott személyről jogsértő deepfake tartalmak közzététele adott esetben a becsület, a magánszféra vagy az „image jogok" (angolul: „*right to publicty*") megsértésével járhat.[194] Megjegyzendő továbbá, hogy az elmúlt időszakban az automatizált döntéshozatallal és az MI egyes káros vagy kockázatos alkalmazásainak kiküszöbölésével kapcsolatos szabályozás a szövetségi szint mellett tagállami szinten is jelentősnek mondható lendületet vett. E tekintetben a kaliforniai szabályozás szintén kiemelt jelentőséggel bír, e körbe értve az AB 331. sz. törvény-tervezetet,[195] amely az automatizált döntéshozatali eszközökkel

[187] AIRIA, sec. 201(10)
[188] AIRIA, sec. 201(6)
[189] AIRIA, sec. 201(4)(B)
[190] AIRIA, sec. 206
[191] AIRIA, sec. 207
[192] AIRIA, sec. 203
[193] AIRIA, sec. 202
[194] Jason HAAS: Deepfake dilemma. Intellectual property magazine, 2044-7175. (September 2019) 33
[195] Assembly Bill No. 331, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=202320240AB331&version=20230AB33195AMD

kapcsolatban ír elő követelményeket. A fentieken túl Kalifornia állam a félrevezető, ún. deepfake tartalmakkal szemben is több szempontból példamutatónak tekinthető szabályozást vezetett be. A 2023. január 1-ig hatályban lévő, AB 730. sz. törvény[196] a deepfake tartalmak választási manipuláció érdekében történő felhasználását tilalmazta (ideértve például: egy jelöltet negatív színben feltüntető hamis felvétel nyilvánosságra hozatala), míg az AB 602. sz. törvény[197] digitálisan, illetve elektronikus úton készített félrevezető és rosszindulatú szexuális tartalmú felvételek (például: zsarolás vagy lejáratás céljából készített hamis pornográf felvételek) felhasználásával szemben lép fel, illetve helyez kilátásba szankciókat (ideértve szabadságvesztés büntetést is). Hasonló törvény-tervezet került benyújtásra Pennsylvania államban is, amely szintén szankcionálni kívánja az MI által létrehozott, mások érdekeit sértő, manipulált szexuális tartalmakat.[198]

A fentieken túl több állam, ideértve például az automatizált munkavállalói döntéshozatal alkalmazása kapcsán New York államot,[199] az MI munkahelyi célú alkalmazásának átláthatósága kapcsán Massachusetts államot,[200] valamint az MI videóinterjúk során történő alkalmazása kapcsán Illinois államot,[201] a munkahelyi adatkezelések kapcsán is bevezetett automatizált döntéshozatallal kapcsolatos szabályokat, tekintettel arra, hogy ezen területeken a munkaviszonyban gyengébb félnek tekinthető munkavállalók védelme erőteljesebb szabályozást követelt meg.

A fentieken túl számos egyéb területen is aktívabbnak tekinthető az MI fókuszú amerikai tagállami szabályozás, ideértve – többek között – az egészségügy vagy a biztosítási szolgáltatások területét, illetve az MI általi diszkriminációt.[202] Ezen szabályok számos esetben tartalmaznak adatvédelmi szempontból jelentős rendelkezéseket, például: a technológia alkalmazásával és az MI általi adatkezelés átláthatóságával kapcsolatos követelményeket,

[196] Assembly Bill No. 730, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201920200AB730&version=20190AB73093CHP
[197] Assembly Bill No. 602, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602
[198] House Bill 1063, https://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2023&sind=0&body=H&type=B&bn=1063
[199] Local Law 144 of 2021 regarding automated employment decision tools ("**NY Local Law 144**"), https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page
[200] An Act Preventing a Dystopian Work Environment (H.1873), https://malegislature.gov/Bills/193/H1873
[201] Artificial Intelligence Video Interview Act, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68
[202] Lásd: Electronic Privacy Information Center, The State of State AI Laws: 2023, 2023.08.03., https://epic.org/the-state-of-state-ai-laws-2023/

azonban sok esetben egyéb, társadalmilag jelentős szempontokat is kiemelnek (például: diszkrimináció tilalma, munkavállalók vagy betegek érdekeinek védelme). Erre tekintettel a jövőben vélhetőleg növekvő számú MI fókuszú jogszabállyal számolhatunk, amelyek számos iparág, illetve terület kapcsán fogják az érintettek jogait és szabadságait szélesebb körű védelemben részesíteni, valamint a technológia etikus felhasználásának követelményeit erősíteni.

d. A mesterséges intelligencia szabályozása az európai és amerikai szabályozáson túl

Természetesen az Európai Unión és az Amerikai Egyesült Államokon túl a világ számos egyéb országában is jelentős változások történtek az MI szabályozása területén, a világ vezető gazdaságainak jelentős része pedig már megalkotta saját MI stratégiáját, némely országok pedig az európaihoz vagy az amerikaihoz hasonló módon, konkrét szabályozási környezet kialakításába is kezdtek. Az MI szabályozáson túl természetesen az adatvédelem területén is számos ország saját szabályozást alakított ki, sok esetben az európai szabályozási megközelítéseket (ideértve különösen a GDPR szabályait) alapul véve.

Az Egyesült Királyság például átfogó célkitűzéseket határozott meg az MI online térben való szabályozás érdekében a 2019-ben publikált „*Online Harms Whitepaper*" elnevezésű dokumentumban. A dokumentum célul tűzi ki egy biztonságosabb internet megteremtését, valamint egyes online szolgáltatók felelős megatartását és ennek kapcsán konkrét lépések megtételét, amely kiterjed például a visszaélések vagy dezinformáció céljára alkalmazott MI alapú megoldások elleni fellépésre is.[203] A fentieken túl 2023. márciusában az Egyesült Királyság kormánya megjelentetett egy újabb, „*A pro-innovation approach to AI regulation*" elnevezésű dokumentumot,[204] amelyben egyrészt áttekinti a jelenlegi szabályozási helyzetet, valamint az innováció előmozdítását is figyelembe vevő további észrevételeket és javaslatokat fogalmaz meg az MI szabályozás területén. A dokumentum továbbá konkrét lépéseket is ígér a fentiek megvalósítása érdekében, ideértve – többek között – széleskörű konzultáció

[203] HM Government, Online Harms Whitepaper, 2019. április, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf, lásd különösen: 6, 23-24

[204] Department for Science, Innovation & Technology, A pro-innovation approach to AI regulation, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1176103/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf

lefolytatását, ennek eredményei összefoglalását, szabályozás felvázolását, szabályozási akadályok azonosítását és az MI-vel kapcsolatos kockázatok felmérésével és jelentésével kapcsolatos jó gyakorlatok kialakítását a fenti dokumentum megjelenését követő 6 hónapon belül.[205] Emellett a következő 12 hónapon belül ígéri a dokumentum kapcsán vezető szervezetek közti együttműködési megállapodások jóváhagyását, a vezető szabályozó szervek támogatását iránymutatások kiadására, valamint központi keretrendszer kidolgozását, amely kitér többek között az MI-vel kapcsolatos adatforrásokra is.[206] Mindemellett a fenti dokumentum hosszútávú célokat is meghatároz, ideértve – többek között – egy kockázati alapú MI nyilvántartás, valamint szabályozói tesztkörnyezet kialakítását.[207]

A fentieken túl az adattovábbítások területén is a közelmúltban olyan fejleményeknek lehettünk tanúi, amelyek az MI általi adatkezeléseket is befolyásolhatják. Így a Brexit-et, azaz az Egyesült Királyság Európai Unióból való kilépését követően az Európai Bizottság megfelelőségi határozatot adott ki, amelyben az EU-ból az Egyesült Királyságba történő adattovábbítást megfelelőnek tekintette mind a GDPR által szabályozott,[208] mind a bűnügyi adatvédelmi irányelv[209] által érintett adattovábbítások tekintetében. Ennek keretében akár MI célú kutatások, valamint egyéb MI általi adatkezelések megvalósítása érdekében történő adattovábbításokra is könnyebben kerülhet sor az EU-ból az Egyesült Királyság területére (például: kutatóintézetek vagy gyógyszeripari vállalatok részére).

A fentiek mellett nemrég megjelent az MI-rendszerek tekintetében átfogó szabályozást kínáló Artificial Intelligence (Regulation) Bill nevű jogszabály tervezete is, amely az MI megoldások fejlesztésével, alkalmazásával, szabályozásával kapcsolatosan MI hatóság létrehozásáról határoz, emellett követelményeket határoz meg az MI megoldások fejlesztői, alkalmazói

[205] A pro-innovation approach to AI regulation, 72–73.
[206] A pro-innovation approach to AI regulation, 73.
[207] Uo.
[208] A Bizottság (EU) 2021/1772 végrehajtási határozata (2021. június 28.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről (az értesítés a C(2021) 4800. számú dokumentummal történt) (EGT-vonatkozású szöveg), C/2021/4800, HL L 360., 2021.10.11, p. 1–68 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[209] A Bizottság (EU) 2021/1773 végrehajtási határozata (2021. június 28.) az (EU) 2016/680 európai parlamenti és tanácsi irányelv szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről (az értesítés a C(2021) 4801. számú dokumentummal történt), C/2021/4801, HL L 360., 2021.10.11, p. 69–107 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

számára, ideértve például az átláthatósággal, biztonsággal, források megjelölésével kapcsolatos követelményeket.[210]

A fentiekhez hasonlóan, adattovábbítási szempontból Kanadát is megfelelőnek minősítette az Európai Bizottság, közel két évtizeddel korábban, 2001. decemberében meghozott döntésében,[211] amely azonban kizárólag a gazdasági szereplők részére történő adattovábbítások körére terjed ki, a közszféra szereplői részére történő adattovábbításokra nem, e tekintetben külön megfelelő garanciák biztosítása szükséges az EU-ból történő adattovábbításokhoz. Kanada emellett 2017-ben hirdette meg MI stratégiáját, jelentős hangsúllyal a kutatások és fejlesztések ösztönzésére, valamint a megfelelő szakértői bázis kialakítására.[212] Emellett megemlítendő, hogy 2022-ben benyújtásra került egy törvény-csomag[213] a kanadai törvény-hozásban, amely magában foglalja a fogyasztói adatvédelmet erősítő „Consumer Privacy Protection Act" elnevezésű törvény-tervezetet, az egyes adatvédelmi kérdésekben benyújtott jogorvoslatok elbírálásául szolgáló fórum felállítását megteremtő „Personal Information and Data Protection Tribunal Act", valamint az „Artificial Intelligence and Data Act" elnevezésű törvény-tervezeteket. Ez utóbbi különösen a nagy kockázatú MI-rendszerek tervezése, fejlesztése és alkalmazása kapcsán rögzít követelményeket, továbbá egyéb, például megfelelő átláthatóság biztosítását, jó gyakorlatok megteremtését célzó rendelkezést is tartalmaz.

A fentiek kapcsán szintén említésre méltó a digitalizációs és MI szabályozás területén a Kínai Népköztársaság szabályozási megközelítése, figyelembe véve, hogy az utóbbi időszakban ezen területeken Kína különösen aktívnak mutatkozik. Mindez azért is tekinthető lényeges szempontnak, mivel Kína ezeken a területeken ezt megelőzően az átfogó szabályozástól helyett inkább a gazdasági és a technológiai fejlődésre fókuszált, látszólag mintegy „kihasználva" a szabályozatlan piaci környezetet, valamint a nyugatitól eltérőnek tekinthető társadalmi berendezkedését. A nyugati sajtóban például gyakran jelentős visszhangot kap a társadalmi pontrendszer és a kormányzat szempontjából nem megfelelőnek ítélt állampolgárok esetleges

[210] Artificial Intelligence (Regulation) Bill [HL], https://bills.parliament.uk/publications/53068/documents/4030
[211] A Bizottság határozata (2001. december 20.) a 95/46/EK európai parlamenti és tanácsi határozat értelmében a személyes adatoknak a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő védelméről (az értesítés a C(2001) 4539. számú dokumentummal történt), HL L 2., 2002.1.4, p. 13–16 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)
[212] OECD.AI, Pan-Canadian AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-14828
[213] Parliament of Canada, BILL C-27, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

elvágása bizonyos szolgáltatásoktól (például: repülő- vagy vonatjegy vásárlása).[214] Mindez a Kínai Népköztársaságban már 2014-től alkalmazott társadalmi pontozási rendszeren alapul, amely segítségével a kínai kormányzat értékelni tudja az állampolgárokat (ideértve azt is, hogy kit tekint „jó polgárnak") a róluk tárolt, illetve kezelt hatalmas mennyiségű információ alapján.[215] Ezzel összhangban a kínai kormány jellemzően az állampolgárok internethasználatát is igyekszik korlátozni, illetve megfigyelni az internetszuverenitás elvéből, és így a sajátos kínai internet kialakításának és szabályozásának gondolatából kiindulva.[216]

A fenti aggályosnak tekinthető megoldásokon túl a kínai szabályozási fejlődési ívnek része volt a 2017-ben hozott átfogó kínai kibervédelmi szabályozás, majd a 2021-es kínai adatvédelmi törvény, ezt pedig egy átfogó MI-t szabályozó törvény meghirdetése követte.[217] Ezt követően 2023-ban a kínai kormányzat generatív MI alkalmazásokkal kapcsolatos átmeneti intézkedéseket adott ki, amelyben egyben a technológiai fejlődés támogatását is célul tűzte ki, valamint a befektetők és üzleti körök megnyugtatását is célozta.[218] A fentiekre tekintettel látható, hogy a technológia és a digitalizáció területén Kína immár nemcsak gazdasági, hanem szabályozói szereplőként is egyre aktívabban kíván megjelenni.

A fentieken túl természetesen számos egyéb ország is alkotott MI fókuszú nemzeti stratégiát vagy vezetett be bizonyos MI fókuszú szabályozást. A fentebb említett, illetve az esetleges egyéb országok szabályozásának bővebb tárgyalása, valamint valamennyi ország szabályozási megközelítésének kifejtése, összevetése azonban túlmutatna a jelen értekezés célkitűzésein és észszerű terjedelmi korlátjain, így attól a továbbiakban eltekintünk.

e. A technológiai nagyvállalatok önszabályozása

Az állami szereplők, valamint a nemzetközi szervezetek MI stratégiái, etikai iránymutatásai mellett szükségesnek látszik szót ejteni a technológiai szektor MI szabályozással, valamint

[214] Nicole KOBIE: The complicated truth about China's social credit system. *Wired*, 2019.06.07. https://www.wired.co.uk/article/china-social-credit-system-explained
[215] BARTNECK-LÜTGE-WAGNER-WELSH op. cit. 69.
[216] GOSZTONYI Gergely: A kínai internetcenzúra modellje. *Pro Futuro*, 2022/1, https://doi.org/10.26521/profuturo/2022/1/11118. 28.
[217] Matt SHEEHAN: China's AI Regulations and How They Get Made, July 2023, Carnegie Endowment for International Peace, https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf. 9, 24
[218] Angela Huyue ZHANG: The Promise and Perils of China's Regulation of Artificial Intelligence, University of Hong Kong Faculty of Law Research Paper No. 2024/02. (January 28, 2024), https://ssrn.com/abstract=4708676, http://dx.doi.org/10.2139/ssrn.4708676. 20.

etikai irányelvekkel kapcsolatos szempontjairól, tekintettel arra, hogy az iparági szereplők a piaci meglátásokat és a szabályozás gyakorlati alkalmazásával kapcsolatos egyes szempontokat sok esetben saját tapasztalataikra, technológiai és gazdasági ismereteikre építve tudják megjeleníteni. Ráadásul a web 2.0 korában a felhasználók immár a tartalomfelhasználás és gyártás aktív részeseivé váltak, így számos adatot osztanak meg, illetve állítanak elő közösségi médiaoldalakon, valamint egyéb platformokon, applikációkon vagy internetes szolgáltatások igénybevételén keresztül,[219] amelyre a technológiai vállalkozások is támaszkodnak szolgáltatásaik nyújtása és fejlesztése során. Mindez pedig egy olyan adatvagyont eredményez, amelynek révén a legnagyobb technológiai vállalatok jelentős előnyre tudnak szert tenni az MI megoldások fejlesztése során. A technológiai szektor szereplői által kidolgozott, illetve kitűzött alapelvek és szempontok így tükrözik ugyan ezen vállalatok gazdasági érdekeit, azonban – mint azt az alábbiak szerint is látni fogjuk – az esetek döntő többségében a demokratikus államok és nemzetközi szervezetek alapvetéseivel és meglátásaival is sok szempontból egyeznek, illetve azokkal összhangba hozhatók. A technológiai szektor önszabályozásának ismertetése kapcsán három, az MI fejlesztések területén kiemelkedő eredményekkel és piaci részesedéssel bíró amerikai technológiai nagyvállalat (Google, Meta, Microsoft) szabályozását és vonatkozó nyilvános kommunikációit vettük górcső alá, és azokat az alábbiak szerint ismertetjük.

Az amerikai technológiai nagyvállalatok közül a Google kiemelten jelentősnek mondható az MI alkalmazások nagyközönség számára való terjesztése, illetve e célból való rendelkezésre bocsátása tekintetében. Erre jó példának tekinthető a Google Bard elnevezésű MI-alapú alkalmazás,[220] amely a ChatGPT-hez hasonlóan, általános segítő alkalmazásként szolgál. A Google az MI fejlesztése és alkalmazása kapcsán többféle alapelvet, illetve alapkövetelményeket is meghatározott, e körbe értve az MI alapú alkalmazások fejlesztésének céljait, illetve olyan alkalmazásokat, amelyek megalkotását, illetve használatát egyáltalán nem célozza. Így a Google az MI alapú alkalmazások kapcsán az alábbi célokat határozta meg:

- társadalmi hasznosság,
- az igazságtalan elfogultság elkerülése,
- biztonságosként építve és tesztelve,
- elszámoltathatónak lenni az emberek felé,
- beépített adatvédelmi alapelvek,

[219] TÓTH András: A web 2.0 versenyjogi vonatkozásai: In: KLEIN Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről*. Médiatudomány Intézet, 2018. 51. [a továbbiakban: TÓTH (2018)]
[220] Google, Bard Experiment, https://bard.google.com/?hl=en

- magas szintű tudományos színvonal fenntartása,
- a fenti alapelveknek megfelelő használatra való elérhetővé tétel.[221]

A Google továbbá azon MI alapú alkalmazásokat is meghatározta, amelyeket nem készül sem fejleszteni, sem alkalmazni, ideértve a különböző aránytalan károkat okozó, fegyverként használható vagy tiltott megfigyelésre szolgáló, illetve nemzetközi jogi, emberi jogi alapelveket sértő technológiákat.[222] Mindennek tükrében tehát a Google kiemelkedőnek tartja a társadalom számára hasznos, a társadalmi igazságosságot előmozdító MI alapú megoldások létrehozását, amelyek egyben magas tudományos színvonalat képviselnek, valamint biztonságosak, és a személyes adatok jogszerű kezelése révén kerülnek alkalmazásra. A biztonságos megoldások alkalmazása a gyakorlatban szintén különös jelentőséggel bír, tekintettel arra, hogy a felhasználók alkalmazhatnak különböző, személyes adatok védelmét erősíti megoldásokat (például: VPN vagy titkosítás), azonban ezen megoldások nem mindig hatékonyak vagy elégségesek.[223]

A Google továbbá „*Perspectives on issues in AI governance*" elnevezésű dokumentumában egyéb olyan szempontokat is összefoglalt, ahol egyértelmű szabályozói gyakorlatra, valamint határozott iránymutatásokra van szükség a megfelelő MI fejlesztői és alkalmazói környezet kialakítása érdekében. Így a Google a fenti dokumentumában kiemelten fontosnak tartja a megmagyarázható MI-vel (angolul: „*explainable AI*")[224] kapcsolatos jó gyakorlatok, esetek, példák, minimum elvárások egyértelmű meghatározását, az MI megfelelőségével kapcsolatos egyértelmű keretrendszer és szempontok felállítását, továbbá a biztonsági szempontokkal kapcsolatos alapvető munkafolyamatok, dokumentációs követelmények, biztonsági tanúsítványok meghatározását.[225] Mindemellett a fenti dokumentum hangsúlyozza az MI-vel kapcsolatos munkafolyamatok kapcsán az emberi részvétel szükségességével kapcsolatos helyzetek pontosítását, valamint az emberi felülvizsgálattal kapcsolatos különböző

[221] Google AI, Our Principles, https://ai.google/responsibility/principles/
[222] Uo.
[223] Karl MANHEIM, Lyric KAPLAN: *Artificial Intelligence: Risks to Privacy and Democracy*. Yale Journal of Law & Technology, vol. 21., no. 106. (2019) 124.
[224] Ideértve az olyan eszközöket és keretrendszert, amelyek segítségével megmagyarázhatók, illetve előre láthatók vagy tervezhetők az MI által hozott döntések, lásd: Explainable AI, Google, https://cloud.google.com/explainable-ai
[225] Google, Perspectives on Issues in AI Governance, https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf. 5.

megközelítések, helyzetek felmérését, felelősséggel kapcsolatos szabályozás, szektorspecifikus szempontok, kivételek és felelősségkorlátozás számbavételét.[226]

A Google emellett az MI szabályozás kapcsán, valamint az MI szabályozás átültetésével kapcsolatos gyakorlati szempontok vonatkozásában is számottevő javaslatokat tesz. Így az MI szabályozás általános megközelítése kapcsán a Google az alábbiakat emeli ki:

- szektorális megközelítés alkalmazása, amely már meglévő szabályozásra épít,
- arányos, kockázatalapú keretrendszer meghatározása,
- az MI-re vonatkozó szabványok és szabályozás interoperábilis megközelítésének előmozdítása,
- az MI alapú, valamint egyéb, nem MI-alapú rendszerek közti elvárások egyenlőségének biztosítása,
- az átláthatóság problémamegoldó képességének elismerése.[227]

A fentiek mellett a Google a szabályozás átültetésével kapcsolatos gyakorlati szempontokat is meghatároz, ideértve az alábbiakat:

- a kockázatértékelések elvégzésével kapcsolatos elvárások tisztázása,
- a nyilvánosságra hozatali követelményekkel kapcsolatos pragmatikus megközelítés alkalmazása,
- a megmagyarázhatósággal és a reprodukálhatósággal kapcsolatos működő normák, illetve szabványok létrehozásához megegyezés szükséges,
- az ex-ante auditnak a folyamatokra kell fókuszálnia,
- annak biztosítása, hogy a megfelelőséggel kapcsolatos referenciaértékek hasznosak legyenek, az alkalmazás tágabb környezetét is figyelembe véve,
- a megbízhatóság priorizálása az adott helyzetben elvárhatóan,
- az emberi felülvizsgálatra való túlzott támaszkodással kapcsolatos óvatosság az MI-vel kapcsolatos problémák kezelése területén.[228]

A fentiek alapján tehát a Google kiemelten fontosnak tekinti – az általános szabályozással szemben álló megközelítést követő – szektorális szabályozást, valamint a kockázatalapú

[226] Uo.
[227] Google, Recommendations for Regulating AI, https://ai.google/static/documents/recommendations-for-regulating-ai.pdf. 2-5.
[228] Google, Recommendations for Regulating AI, 6-16.

megközelítést és az interoperabilitást. Emellett egyenlő elvárásokat kíván meg az MI alapú és nem MI alapú rendszerekkel szemben – mintegy az MI alapú rendszerekkel szembeni esetleges „megkülönböztetéssel" szemben felszólalva –, és ugyancsak hangsúlyozza az átláthatóság fontosságát, amely az európai adatvédelmi szabályozás tükrében kétségtelenül lényeges szempontot képvisel, figyelembe véve azt is, hogy a felhasználók jellemzően nincsenek abban a helyzetben, hogy érdemi beleszólásuk legyen a technológiai vállalatok általános szerződési feltételeinek, adatkezelési gyakorlatának érvényesítésébe, amelyet csak elfogadni vagy tudomásul venni tudnak, ha használni kívánják az adott alkalmazást vagy szolgáltatást, [229] így az átláthatóság biztosítása a felhasználók részére jelentősen segítheti helyzetük és jogaik könnyebb megértését, megismerését.

A Meta csoport ugyancsak jelentős lépéseket tett az adatvédelmi megfelelés érdekében. Így a közelmúltban egy részletes jelentést tettek közzé, amelyben összefoglalták ezen adatvédelmi megfeleléssel kapcsolatos lépéseiket és törekvéseiket, ideértve például meghatározott termékek, megoldások adatvédelmi megfelelésével kapcsolatos csoportok („*privacy product groups*") vagy adatvédelmi megfeleléssel kapcsolatos csapatok („*Meta Privacy and Data Practices Team*"), illetve egy negyedévente ülésező, független adatvédelmi bizottság („*Privacy Committee*") felállítását. Emellett a Meta lépéseket tett például az adatvédelmi oktatás, az adatvédelmi kockázatértékelés- és kezelés, valamint az adattovábbítások és azok átláthatósága területén is.[230]

A fentiek mellett a Facebook kapcsán meghatározásra került a felelős MI fejlesztés és alkalmazás öt oszlopa, amelyeket a Facebook esetén a Meta figyelembe vesz, ideértve az alábbiakat:

- adatvédelem és védelem,
- tisztesség és befogadás,
- megbízhatóság és biztonság,
- átláthatóság és irányítás,
- elszámoltathatóság és kormányzás.[231]

[229] MANHEIM, KAPLAN op. cit. 133.
[230] Meta, Privacy progress update, We have a responsibility to protect people's privacy and give them control to make their own choices, https://about.meta.com/privacy-progress?utm_source=about.facebook.com&utm_medium=redirect
[231] Meta AI, Facebook's five pillars of Responsible AI, 2021.06.22, https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/

A fentieken túl a Microsoft technológiai nagyvállalat is meghatározta a felelős MI alapelveit, ideértve az alábbiakat:

- tisztesség,
- megbízhatóság és biztonság,
- adatvédelem és védelem,
- befogadás,
- átláthatóság,
- elszámoltathatóság.[232]

Ahogy azt a fentebb írtakból is láthatjuk, a fentebb írt alapelvek, illetve követelmények jellemzően más piaci szereplők kommunikációiban is megjelennek, ideértve például a Meta csoportot, illetve a Facebook-ot, ezentúl továbbá több esetben olyan általános követelményeket, illetve alapelveket jelenítenek meg, amelyek számos esetben a nemzetközi vagy regionális, illetve nemzeti adatvédelmi szabályozásban is megjelennek (például: tisztesség, átláthatóság, elszámoltathatóság).[233]

Ahogy az a fentiekből is látszik tehát, mind a nemzetközi szervezetek és az egyes államok közösségei, mind a technológiai szektor szereplői számos szempontból hasonlóan határozták meg az MI fejlesztésével, valamint használatával kapcsolatos alapelveket. Mindemellett az MI-vel kapcsolatos szabályozási kezdeményezésekre tekintettel a technológiai nagyvállalatok etikai keretrendszere, valamint a velük való együttműködés jelentős segítséget nyújthat az MI szabályozás kialakítása és megfelelő alkalmazása tekintetében.[234] Habár az egyes szervezetek, szereplők által meghatározott alapelvekben és a kapcsolódó iránymutatásokban „áthallatszanak" az adott szereplők érdekei, emellett az etikai és jogi szempontból is kiemelkedő, alapvető követelmények is megjelennek. Így jellemzően az alábbi alapelvek jelennek meg közös pontként az egyes államok, nemzetközi szervezetek, valamint a technológiai iparág szereplői kommunikációiban, iránymutatásaiban:

- tisztesség,
- az érintettek érdekeinek figyelembevétele,

[232] Microsoft, Putting principles into Practice: How we approach responsible AI at Microsoft, https://www.microsoft.com/cms/api/am/binary/RE4pKH5#:~:text=At%20Microsoft%2C%20we've%20recognized,inclusiveness%2C%20transparency%2C%20and%20accountability. 4–7.
[233] Lásd például a GDPR 5. cikke szerinti alapelveket.
[234] LANE (2022) op. cit. 926–927.

- átláthatóság,
- adatvédelem,
- megbízható és biztonságos alkalmazás,
- kockázatértékelés.

Kiemelendő, hogy bár a fenti alapelvek és alapvető követelmények jellemző módon markánsan megjelennek mind a fentebb említett etikai iránymutatásokban, állásfoglalásokban és egyéb dokumentumokban, természetesen számos egyéb szempont is kiemelhető, amelyek az etikus MI szabályozás, fejlesztés és alkalmazás területén jelentőséggel bírhatnak, emellett az MI alapú fejlesztés, alkalmazás adott körülményeire, szempontjaira, valamint az érintettek körére, az adott szakterületre, iparágra jellemző egyéb, különösnek tekinthető elvárások és alapelvek is meghatározhatók (ideértve például: az MI egészségügyi vagy munkahelyi alkalmazása esetén, hiszen ezen területeken jellemzően sajátos követelményeknek, szempontoknak kell érvényesülniük, amelyek maximálisan figyelembe veszik az érintett érdekeit).

Mint az a fentiekből is látszik, az MI etikus, valamint az alapvető emberi jogi és alkotmányos értékekkel összhangban álló fejlesztése és alkalmazása az egyetlen elfogadható lehetőség, amelyet mind a nemzetközi és nemzeti jogalkotók, mind a legnagyobbnak mondható technológiai és piaci szereplők egyértelmű célul tűztek ki maguk, valamint az emberiség elé. Az etikus MI megoldások emellett jelentős társadalmi támogatottsággal is rendelkeznek, az ezek alkalmazásához tapadó átláthatóság, valamint egyéb emberi jogi, adatvédelmi elveknek és elvárásoknak való megfelelés a technológia megbízhatóságával kapcsolatos félelmek eloszlatását is jelentős mértékben segítheti.[235]

4. A mesterséges intelligencia általi adatkezelés az Európai Unióban

Napjainkra az MI alkalmazása számos területen dominánssá vált, tekintettel arra, hogy mind vállalkozások, mind magánszemélyek, kormányzati és egyéb szervezetek egyre növekvő számban használnak MI alapú alkalmazásokat, és vesznek igénybe vagy nyújtanak kapcsolódó szolgáltatásokat. Ennek kapcsán kijelenthető, hogy az MI az európai gazdaság egyik fő mozgatórugójává vált, mindemellett a társadalmi szokások formálása kapcsán is egyre nagyobb

[235] NECZ Dániel: A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. *Rendvédelem*, 2020/01. 142. [a továbbiakban: NECZ (2020a)]

szerepet kap. Az MI által nyújtott mindezen előny azonban a személyes adatok nagyobb mértékű, kiterjedt kezelésével is jár, és számos területen egyéb társadalmi szempontból jelentős kockázatokkal is bírhat, amelyeket az európai jogalkotó is igyekszik megfelelő módon kezelni, ideértve különösen az etikus MI-alkalmazás keretrendszerének, valamint az MI-rendszerek alkalmazásával kapcsolatos felelősségi szabályok észszerű és arányos meghatározását.

Természetesen azonban az MI-vel kapcsolatos etikai elvárásokon, valamint felelősségi szabályokon túl kiemelt jelentőséggel bír az MI általi adatkezelés szabályozása és a vonatkozó jogalkalmazói gyakorlat is, tekintettel arra, hogy az MI elsődleges „tápanyagának" az adat tekinthető, amely révén az MI képes eredményeket produkálni, illetve döntéseket hozni, valamint fejlődni. Erre tekintettel szükséges az adatvédelmi szabályokat az MI általi adatkezelés keretében is megfelelően értelmeznünk. Így a jelen fejezetben sor kerül az MI általi adatkezelés alapvető szempontjainak összefoglalására, ideértve különösen az adatkezeléssel kapcsolatos szerepkörök meghatározását, az MI általi adatkezelés átláthatóságával kapcsolatos elvárásokat, az adatkezelés jogalapjával és jogszerűségével kapcsolatos, továbbá az érintetti jogok gyakorlásával kapcsolatos szempontokat. Ennek kapcsán az adatkezelői szerepek között kiemelten tárgyaljuk az adatgazdaságban betöltött jellemző szerepköröket, az ezzel kapcsolatos információmegosztás jelentőségét, amely remélhetőleg több esetben válik elfogadottá, így megteremtve és támogatva az információ hatékony megosztását.[236]

Emellett a jelen fejezetben az MI általi adatkezelés egyéb jelentős szempontjai is összefoglalásra kerülnek, ideértve az adatvédelmi hatásvizsgálat elvégzésével, az adatvédelmi tisztviselők kinevezésével, az adatbiztonsággal, az adattovábbítással kapcsolatos szempontokat, valamint a szektorális adatkezeléssel és az adatgazdasággal kapcsolatos egyes kihívásokat. Ennek kapcsán – a tanulmány terjedelmi kereteire tekintettel – az MI valamennyi iparág, illetve szakterület kapcsán végzett alkalmazásának adatvédelmi szempontjai ismertetésétől értelemszerűen eltekintünk, és a társadalom működése szempontjából különösen jelentősnek tekinthető egyes területekre, így az egészségügyi, valamint a munkahelyi adatkezelésre és az MI online platformokon való alkalmazására fókuszálunk. Természetesen az MI alkalmazását és annak adatvédelmi szempontjait számos területen jelentősnek tartjuk (ideértve például: a közlekedést, az ipari célú vagy az oktatási célú, illetve szociális alkalmazást), azonban az értekezés vonatkozó részeiben olyan szektorális szempontok

[236] PÓK (2022) i.m. 397.

megragadására törekedtünk, amelyek különösen közeli kapcsolatba hozzák az MI-t az emberrel, és napjainkban társadalmi, továbbá adatvédelmi szempontból is kiemelt jelentőséggel bírnak. Ennek kapcsán azonban kiemelendő, hogy a tanulmány egyéb részeiben az MI egyéb területeken való alkalmazásával is foglalkozunk, valamint alább külön fejezetben tárgyaljuk az MI és az adatvédelem további kihívásait, amelyek területén az adatvédelmi elvárások a közeljövőben vélhetőleg egyre nagyobb hangsúllyal bírnak majd.

a. A személyes adatok és a mesterséges intelligencia

Az MI szabályozásával kapcsolatos kihívások számos esetben a személyes adatok kezelésével, valamint az MI sokszor csillapíthatatlannak látszó adatéhségével hozhatók összefüggésbe. Az MI által felhasznált adatok azonban sok esetben nem személyes vagy épp közérdekű,[237] továbbá – a lényegében „hungarikumnak tekinthető" – közérdekből nyilvános adatok[238] kezelését foglalják magukban, amelyekre nem terjed ki a személyes adatok védelme. A közérdekből nyilvános adatok esetén azonban ez csak azon esetekre igaz, amikor a közérdekű céllal összefüggésben történik az adatkezelés, azonban ezen adatok tekintetében is alkalmazandó a célhoz kötött adatkezelés elve, és személyes adatként védettek lehetnek (például, amennyiben egyéb, a közérdekű, nyilvánosságra hozatalra okot adó céltól eltérő célból kezelik őket).[239] A közérdekű, valamint a közérdekből nyilvános adatok kezelése, valamint az információszabadság megteremtése egyúttal erősíti a közhatalom gyakorlói, valamint a közpénzzel gazdálkodó szervezetek elszámoltathatóságát, és az államszervezet transzparens és hatékony működését.[240]

[237] Magyarországon az Infotv. a közérdekű adatot az alábbiak szerint határozza meg: „*az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat*" (Infotv. 3. § 5. pontja).

[238] Magyarországon az Infotv. a közérdekből nyilvános adatot az alábbiak szerint határozza meg: „*a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli*" (Infotv. 3. § 6. pontja).

[239] A Fővárosi Ítélőtábla Pf.20258/2023/4. számú határozata [58] bek.

[240] KOMANOVICS ADRIENNE: *Információszabadság az Európai Unióban*, Budapest-Pécs, Dialóg Campus Kiadó, 2009. 13.

A fentiek mellett azonban az MI általi adatkezelés bizonyos esetekben érinthet akár szenzitívnek tekinthető adatokat, azaz a személyes adatok ún. különleges kategóriáit is, [241] amelyek csak meghatározott feltételek esetén kezelhetők.[242] Az MI általi adatkezelés érinthet továbbá bűnügyi személyes adatokat is, amelyek szintén csak az uniós vagy tagállami jog által biztosított megfelelő garanciák esetén kezelhetők.[243] Külön szabályozási rezsim vonatkozik továbbá a büntető igazságszolgáltatás körében folytatott a bűnügyi adatkezelésekre, amelynek az EU-n belül a bűnügyi adatvédelmi irányelvet („**Bűnügyi Adatvédelmi Irányelv**")[244] átültető tagállami jogszabályok biztosítanak keretet. Tekintettel arra, hogy a jelen értekezésnek ezen adatkezelések kevéssé képezik fókuszát, így a jelen értekezésben főként a személyes adatok, illetve az ennek körébe tartozó különleges adatok MI általi kezelésére fókuszálunk.

Annak meghatározása azonban, hogy mi tekinthető személyes adatnak, a gyakorlatban sokszor korántsem egyszerű feladat. A GDPR a személyes adat fogalmát tágan határozza meg, e körbe értve az azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információt. Ez utóbbi tekintetében a GDPR további támpontot ad, meghatározva, miszerint „*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*".[245] E tekintetben tehát ugyan tág megfogalmazást alkalmaz a GDPR, azonban számos olyan példaként említett szempontot nevesít, amelyek alapján adott esetben könnyebben állapíthatjuk meg, hogy egy bizonyos információ alapján az érintett legalább közvetett módon azonosítható-e. A fentiek nem jelentenek azonban minden esetben egyértelmű támpontot, ugyanis sem a GDPR, sem az azt megelőző adatvédelmi irányelv nem nyújtott a tekintetben további eligazítást, hogy az adott

[241] E körbe tartoznak a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok. (GDPR 9. cikk (2) bek.)
[242] GDPR 9. cikk (1) bek.
[243] A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelésére „*kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi*". (GDPR 10. cikk)
[244] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4, p. 89–131 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV), III. fejezet („**GDPR**")
[245] GDPR 4. cikk 1. pontja

információ hogyan kapcsolódhat az érintetthez, és így hogyan azonosíthatja őt, ekként pedig sokszor csak esetről-esetre, az adott eset körülményeinek figyelembevétele alapján állapítható meg, hogy az adott információ inkább a védendő személyes adatok körébe tartozónak, vagy egyéb, nem védett információnak tekinthető-e.[246]

A fentiekkel összhangban, a gyakorlatban a személyes adat jellegének megállapítása kapcsán a legfőbb kihívást az érintett adott információ általi azonosítása jelenti. Az Európai Unió Bíróságának („**EUB**”) e körben irányadó gyakorlata értelmében akkor minősül az információ az érintett személyre vonatkozónak, és így az érintett személyes adatának, amennyiben „*az információ tartalmánál, céljánál vagy hatásánál fogva egy meghatározott személyhez kapcsolódik*”.[247] Mindez összhangban van az Adatvédelmi Munkacsoport személyes adat koncepciójáról szóló véleményével, amely szerint az információ „tartalma”, „célja” vagy „eredménye” kapcsán tekinthető az érintettet azonosítónak.[248] Erre tekintettel például személyes adatnak tekinthető az érintett nevét tartalmazó e-mail cím (abban az esetben is, ha ez más adattal együtt azonosítja az érintettet),[249] a dinamikus IP cím[250] vagy a MAC cím,[251] a kutya neve ha az a tulajdonosát azonosítja,[252] vagy akár más személyre, például az élettársra, házastársra vonatkozó információk (mivel azok alapján az érintett szexuális irányultságára vonatkozó információk mint különleges adatok is megismerhetők).[253] Megemlítendő továbbá, hogy az érintettre vonatkozó információk valóságtartalmuktól függetlenül tekinthetők személyes adatnak, ha azok alapján az érintett azonosítható (ideértve például az érintettet meg nem történt események körében bemutató deepfake felvételeket). Kiemelendő azonban, hogy az Adatvédelmi Munkacsoport személyes adatról szóló fenti véleményét az EDPB már nem

[246] Nadezhda PURTOVA: The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, vol. 10., issue 1. (2018). https://doi.org/10.1080/17579961.2018.1452176. 44.
[247] C-434/16. sz. ügy Peter Nowak kontra Data Protection Commissioner [ECLI:EU:C:2017:994] 35. pont
[248] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, Adopted on 20 June, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. 10.
[249] BH 2023.3.65. [19].
[250] C-582/14. sz. ügy Patrick Breyer kontra Bundesrepublik Deutschland [ECLI:EU:C:2016:779] 49. pont
[251] ICO, Can we identify an individual indirectly from the information we have (together with other available information)?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/can-we-identify-an-individual-indirectly/
[252] ICO, Freedom of Information Act 2000 (FOIA) Decision Notice, Information Commissioner's Office (“**ICO**”), 2022.02.08, https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4019607/ic-80804-j7c6.pdf. 6.
[253] C-184/20. sz. ügy OT kontra Vyriausioji tarnybinės etikos komisija [ECLI:EU:C:2022:601] 119. pont

tartotta fenn,[254] így annak meglátásai ugyan bizonyos esetekben továbbra is relevánsnak tekinthetők, azonban a gyakorlatban korlátozottabban érvényesülhetnek.

Ahogy az a fentebb írtakból is következik, számos esetben jelent kihívást az érintett azonosíthatóságával kapcsolatban a személyes adat jellegének megállapítása. Ennek kapcsán a gyakorlatban az adat és az érintett közti kapcsolat helyreállíthatósága alapján az ún. abszolút és relatív elméleteket, illetve megközelítést különböztethetjük meg, annak figyelembevételével, hogy az érintett azonosításához kizárólag az adatkezelőnél vagy adott esetben csak más személyeknél rendelkezésre álló további információk alapján azonosítható-e az érintett.[255] Ennek kapcsán az Európai Unió Bírósága („**EUB**") a fentebb idézett korábbi, főként abszolút elméletet alátámasztani látszó gyakorlatát követően az elmúlt időszakban fokozatosan mozdult el a személyes adat fogalmának relatív értelmezése felé. Ennek kapcsán például az EUB a T-557/20. sz. ügyben hozott döntésében különös súllyal vizsgálta anonim adatok vonatkozásában az érintett újbóli azonosíthatóságának kockázatát, és arra a megállapításra jutott, hogy „*nem teljesülnek a Bíróság ítélkezési gyakorlatában az újbóli azonosítás kockázatának fennállására vonatkozóan támasztott feltételek, amennyiben az azonosítást lehetővé tevő valamennyi információ nem egyetlen személy, hanem több fél birtokában van*".[256] Így amennyiben ugyan az adatkezelő hipotetikusan, több más, az adatkezelő számára el nem érhető információval együtt lenne csak képes az érintett azonosítására, úgy az adatkezelő birtokában lévő adat nem tekinthető személyes adatnak, annak alapján ugyanis az adatkezelő nincs abban a helyzetben, hogy az érintettet azonosíthassa. Ez a logika alkalmazható az ún. álnevesített adatok[257] (például: egy adatkészlet kóddal vagy jelszóval való ellátása az illetéktelen személyek általi hozzáférés megakadályozása érdekében) esetén is, ugyanis itt azon esetekben, ha az adatkezelő nem rendelkezik az álnevesítés feloldására szolgáló kóddal, jelszóval, más megoldással vagy eszközzel, személyes adatról csak kérdésesen beszélhetünk.[258] Ezen megközelítés azonban

[254] EDPB, Endorsed WP29 Guidelines, https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

[255] Az abszolút és a relatív elmélet közötti különbségek ismertetéséhez lásd: CZAPÁRI Dóra, SZŐKE Gergely László: Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása. *JURA*, 2022/4. 28–29.

[256] T-557/20. sz. ügy Egységes Szanálási Testület kontra európai adatvédelmi biztos [ECLI:EU:T:2023:219] 78. pont

[257] A GDPR 4. cikk 5. pontja szerint álnevesítés: „*a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni*".

[258] Lásd: a Törvényszék T-557/20. sz. ügyben hozott ítélete, 99. pont

értelemszerűen az adatkezelő szemszögéből indul ki. Az álnevesített adatok ugyanis megőrzik személyes adat jellegüket, azok adatkezelő általi elérhetetlensége és az érintett azonosításának képtelensége azonban jellemzően szükségtelenné teszik az azonosítható érintetthez kapcsolódó személyes adatokhoz hasonló szintű védelmet.

A gyakorlatban azonban felmerülhetnek olyan esetek is, ahol nehéz meghúzni a határt az érintettre vonatkozó vagy egyéb, nem személyes adatok között. Az ilyen adatok felhasználásához, illetve nyilvánosságához továbbá jellemzően gazdasági vagy társadalmi érdekek is fűződnek. A gyakorlatban például kivételnek tekinthetők a személyes adatok köre alól a jogi személyekre vonatkozó egyes információk, adott esetben azonban az ilyen információk is tekinthetők személyes adatnak, ha azok az érintettet azonosítják. E tekintetben ugyanakkor az EU-n belül egységes és következetes joggyakorlatról nem beszélhetünk. A magunk részéről a német adatvédelmi hatósági gyakorlattal értünk egyet. Ennek tükrében egy egyszemélyes társaság vagy hasonló egyszemélyes szervezet esetén a szervezetre vonatkozó (például: vagyoni, pénzügyi) információk az érintettre vonatkozó személyes adatoknak is betudhatók, különösen abban az esetben, ha erős személyes, vagyoni kapcsolat mutatható ki a szervezet és annak tagja között.[259] Vitatható azonban az ilyen kapcsolat, amennyiben a tag a jogi személy tartozásaiért korlátolt felelősséggel tartozik.[260] A fentiekre tekintettel helyesnek tekinthető azon értelmezés, amely egyedüli taggal működő szervezetre vonatkozó gazdasági, megbízhatósággal kapcsolatos értékeléseket az egyedüli tag személyes adatának tekinti, különösen azon helyzetekben, ahol szoros személyes kapcsolat áll fenn a szervezet és annak egyedüli tagja között, ezen esetekben ugyanis a fenti adatkezelés egyértelműen azonosítja az egyedüli tagot, valamint alapjaiban kihat annak szakmai megítélésére, megélhetésére is.

A fentiek mellett ugyancsak kérdéses lehet adott esetben a foglalkoztatással kapcsolatos információk megítélése. A munkavállalókat természetesen a munkahelyükön, munkavégzésük során is megilleti a személyes adatok védelme, azonban a munkáltatónak is adott esetben érdeke fűződhet egyes, munkavállalóknak címzett vagy általuk kezelt anyagokhoz. Az ír adatvédelmi

[259] Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Einstieg ins Datenschutzrecht für behördliche Datenschutzbeauftragte, 2018.10.19, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/10/Vortrag-f%C3%BCr-DSB_Verwaltungsschule.pdf. 58., Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2021, https://www.datenschutz-berlin.de/infothek/publikationen/jahresberichte/. 124–125.

[260] Sächsische Datenschutz- und Transparenzbeauftragte, Tätigkeitsbericht, Datenschutz, 2022, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2022.pdf. 34–36.

hatóság (angolul: „*Data Protection Commission*”; röviden: „**DPC**”) például a munkahelyi adatkezelés kapcsán 2023-ban kiadott iránymutatásában hangsúlyozta, miszerint a munkavállalónak munkavállalói minőségében címzett e-mailek tartalma nem tekinthető személyes adatnak, mivel ezen e-mail tartalma munkahelyi kontextushoz kapcsolódik.[261] Az ilyen munkahelyi kötődés azonban esetről-esetről vizsgálandó, elkerülve a munkavállalók adatvédelmi jogainak megsértését, így értelemszerűen nem jelenthető ki, hogy a munkavállalóknak címzett vagy általuk írt e-mailek nem tartalmaznak személyes adatokat.

A fentiek mellett sajátos szempontok érvényesülnek továbbá az elhunyt személyek adatainak kezelése kapcsán, amely adatok tekintetében a GDPR nem biztosít védelmet,[262] azonban a tagállami szabályozás bizonyos szempontból védendőnek minősítheti az elhunytakra vonatkozó egyes információkat, dokumentumokat (például: a halál okára vonatkozó információkat, egészségügyi dokumentációt,[263] elhunyt személyek biztosítására vonatkozó információkat[264]) vagy az elhunyt hozzátartozói, örökösei számára meghatározott rendelkezési, illetve kegyeleti jogokat biztosíthat. Így Magyarországon például az Infotv. értelmében a GDPR hatálya alá tartozó adatkezelési műveletek esetén az érintett halálát követő öt éven belül az elhaltat életében megillető egyes jogokat az érintett által erre kijelölt, illetve meghatalmazott személy, ennek hiányában az első joggyakorlóként fellépő közeli hozzátartozó jogosult érvényesíteni.[265] A fenti jogok természetesen nem az elhunyt részére biztosítanak egyfajta halál utáni jogokat, hanem az elhunyt adatai feletti rendelkezést segítik (ideértve például: közösségi profilok, egyes dokumentumok és nyilvántartások kapcsán történő eljárást), illetve lehetőséget teremtenek az esetleges jogsértő vagy céltalanná vált adatkezelésekkel szembeni fellépésre az elhunyt halálát követő észszerű időn belül. Az ilyen információk emellett hasznosak lehetnek egyes MI alkalmazások fejlesztői, szolgáltatói számára is, például kutatási célú vagy statisztikai felhasználás esetén.

Megjegyzendő továbbá, hogy napjainkban az érintett azonosíthatósága kapcsán különös hangsúllyal merül fel az anonimizált adatok (például: az egyes érintetteket egyedileg nem azonosító kimutatások), technikai azonosítók, okostelefonokra vagy egyéb okoseszközökre és

[261] DPC: Guidance Note. Data Protection in the Workplace: Employer Guidance. April 2023. 4.
[262] GDPR (27) preambulum-bekezdés
[263] Lásd: az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 3/A. § szakasza
[264] Lásd: a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 143. § (3) bekezdése
[265] Infotv. 25. § (1)-(2) bek.

ezek használatára vonatkozó egyes információk felhasználása. Egy 2013-ban publikált amerikai kutatás kimutatta például, hogy a mobiltelefonhasználók 95%-a azonosítható volt négy, a hívás helyére és idejére vonatkozó „pont" alapján,[266] míg egy 2019-ben végzett további amerikai kutatás szerint 15 demográfiai adat alapján Massachusetts állam lakóinak 99,98%-a volt egyedileg azonosítható.[267] A fenti kutatások jól példázzák, hogy sok esetben akár statisztikai adatok vagy önmagukban konkrét érintettekhez nem kapcsolható információk is könnyen vezethetnek meghatározott személyek azonosításához, különösen akkor, ha egyszerre többféle adat kerül értékelésre. Az MI alkalmazása pedig az adatok értékelését, és adott esetben egyes információk érintetthez kapcsolását csak megkönnyíti. Egy 2022-es kutatás során például egy nyilvánosan elérhető adatbázisból közel 30.000 betegről készült több mint 100.000 mellkasi röntgenképet elemeztek képfelismerő MI megoldással, az adott megoldás pedig az esetek 95.55%-ában volt képes felismerni, hogy két röntgenkép ugyanazon betegtől származott.[268] Azonban fontos megértenünk, hogy az MI nem kizárólag megkönnyíti vagy felgyorsítja az érintettek azonosítását. Adott esetben olyan összefüggéseket is képes feltárni, amelyekre nem is gondolnánk. Emellett azonban sajnos hibázhat is, például téves adatokat tulajdonítva egy-egy személynek. 2023-ban például egy ausztrál polgármester felszólította a ChatGPT alkalmazást biztosító OpenAI vállalatot, hogy korrigálja az alkalmazásban róla kezelt adatokat, mivel a ChatGPT tévesen azt állította róla a felhasználóknak, hogy vesztegetés miatt börtönben ült.[269] Értelemszerűen az ilyen esetekben nehéz megállapítani, hogy az MI hogyan jut az érintettel kapcsolatba hozható bizonyos információk azonosítására, és milyen jellemzőket tulajdonít az érintettnek.

A technológiai fejlődés személyes adatok védelmére gyakorolt hatása kapcsán többféle megközelítéssel találkozhatunk a jogirodalomban. Nadhezda Purtova például a személyes és nem személyes adat értelmezésével kapcsolatos, valamint ezek közti különbségtétel – technológiai fejlődés által csak felerősített – nehézségeire tekintettel a személyes adat

[266] Yves-Alexandre de MONTJOYE, César A. HIDALGO, Michel VERLEYSEN, Vincent D. BLONDEL: Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, 3. 1376 (2013). https://doi.org/10.1038/srep01376. 2.
[267] Luc ROCHER, Julien M. HENDRICKX, Yves-Alexandre de MONTJOYE: Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10. 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3. 5.
[268] Kai PACKHÄUSER, Sebastian GÜNDEL, Nicolas MÜNSTER, Christopher SYBEN, Vincent CHRISTLEIN, Andreas MAIER: Deep learning-based patient re-identification is able to exploit the biometric nature of medical chest X-ray data. *Scientific Reports*, 12. 14851 (2022). https://doi.org/10.1038/s41598-022-19045-3. 1.
[269] Byron KAYE: Australian mayor readies world's first defamation lawsuit over ChatGPT content. *Reuters*, 2023.04.05, https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/

koncepciójának feladása mellett érvel, ezek helyett az információ kezelése által okozott hatásokra fókuszálva.[270] Ezen megközelítés tükrében Purtova szerint akár az időjárásra vonatkozó információk is személyes adatnak tekinthetők adott esetben, ha az alkalmazott technológia és a vonatkozó adatkészlet alapján azokból meghatározott személyekre lehet következtetni.[271] Habár ezen meglátások kétségtelenül alappal kérdőjelezik meg a személyes adat hagyományos koncepciójának fenntarthatóságát, azonban – ahogy Raphaël Gellert is hangsúlyozza – ezen megközelítés egyik hangsúlyos pontját a technológiai fejlődés lineáris, egyre gyorsuló üteme, valamint ehhez fűződően az érintett egyre könnyebb azonosíthatósága és az anonimizálás kétségessége képezi; ezen megközelítés azonban a technológiai fejlődés kapcsán túlzóan optimistának tűnhet, az anonimizálást pedig kizárólag technológiai értelemben vizsgálja, nem pedig ennél komplexebb, technológiai-társadalmi jelenségként.[272] Ennek kapcsán érdemes megemlíteni, hogy habár a személyes adatok koncepciójának feladása napjainkban még kérdéses lehet, kétségtelen, hogy a technológiai fejlődés, különösen ideértve az MI fejlődését, alapjaiban kérdőjelezik meg a személyes adatok védelméhez fűződő napjainkban domináns megközelítéseket; mindez pedig a védendő adatok körének szélsőséges tágulásához, és az adatvédelem minőségének gyengüléséhez vezethet.[273]

Florent Thouvenin a fentiekhez hasonlóan hangsúlyozza, miszerint magánszereplők általi adatfelhasználás esetén nem hozhatók fel érvek ennek érintett általi korlátozhatóságára, ha egyébként az adatkezelés nem jár káros hatással az érintettre.[274] Thouvenin továbbá az információs önrendelkezési jog feladását és ehelyett az információs adatvédelem (angolul: „*informational privacy*") fókuszba helyezését javasolja, amely értelmében az érintettek dönthetnének arról, hogy mely információkat tesznek hozzáférhetővé magukról mások számára, azonban az információ további felhasználását már nem korlátozhatják; erre tekintettel nem lenne szüksége az adatkezelőknek valamennyi adatkezelés kapcsán megfelelő jogalapra hivatkozniuk és valamennyi adatvédelmi alapelvnek megfelelniük, az adatkezelés átláthatóságát és biztonságát azonban továbbra is garantálniuk kellene.[275] Ződi Zsolt is amellett érvel ennek kapcsán, hogy az adatvédelem helyett inkább egy „privacy" típusú védelmi

[270] PURTOVA op.cit. 79-80.
[271] PURTOVA op.cit. 57-59.
[272] Raphaël GELLERT: Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, vol. 11., issue 2. (2021) 207.
[273] GELLERT op.cit. 208.
[274] Florent THOUVENIN: Informational Self-Determination: A Convincing Rationale for Data Protection Law?. *JIPITEC,* 12/2021. 255.
[275] Uo.

megközelítésre lenne szükséges átállni, amely nem az adatra, hanem a magánszemélyek jogainak és szabadságainak (különösen: méltóságának, magánéletének) védelmére fókuszálna, ekként a személyes adatok kezelésével kapcsolatos túlszabályozást is elkerülve.[276] Emellett egyes álláspontok szerint a személyes adatok kezelésére a szellemi tulajdonjogok kapcsán alkalmazható felhasználási engedélyekhez (licenciákhoz) hasonló szabályozási rendszert lenne szükséges kialakítani, amelyek segítségével az érintettek különböző engedélyeket adhatnának személyes adataik felhasználására.[277]

A fenti álláspontok jól jelzik a jelenlegi – különösen az európai – adatvédelmi szabályozás fenntarthatóságával kapcsolatos kétségeket és kritikákat. A technológiai fejlődés, különösen ideértve az MI fejlődését, megnöveli az elérhető adatmennyiséget, valamint megkönnyíti az információk feldolgozását és azok hatékonyabb kiaknázását. Erre tekintettel – a fentebb írtakkal is összhangban – vélhetőleg a személyes adatok védelmének abszolút elmélete fog majd újra dominánssá válni, ugyanis egyre kevesebb adatból lesz majd egyre több ember egyre több szempontból megismerhető, ennek okán pedig előbb-utóbb szükség lesz majd a személyes adatok védelmének újragondolására. Álláspontunk szerint e tekintetben a fentiekhez hasonlóan a személyes adatok védelme kapcsán az adatkezelés érintettre gyakorolt hatásaira kellene nagyobb hangsúlyt helyezni a személyes adat koncepciójához való görcsös ragaszkodás és ezzel kapcsolatban az adatvédelmi szabályozás teljeskörű és általános érvényesítése helyett. Ezen megközelítés garantálná az adatvédelmi szabályok arányos érvényesítését, így egyúttal azt is, hogy az érintettek a számukra valóban jelentősnek mondható adatkezelések esetén élvezzenek védelmet. E körben álláspontunk szerint a személyes adatok védelme nem szűkülhet kizárólag a magánélet védelmére, hiszen ezen megközelítés például az érintettek munkavégzésével, szakmai tevékenységével kapcsolatos információkat is védelmen kívül hagyná, a védelem alkalmazhatóságát és minőségét azonban az adatkezelés érintettre gyakorolt hatásaitól kellene függővé tenni, így elkerülve a túlzottan bürokratikus szabályozást és a társadalmi, gazdasági élet szereplői, különösen a kis- és középvállalkozások aránytalan terhelését.

[276] ZŐDI Zsolt: Privacy és a Big Data. *Fundamentum*, 2017/1-2. 28. [a továbbiakban: ZŐDI (2017)]
[277] Lásd: Paul JURCYS, Chris DONEWALD, Jure GLOBOCNIK, Markus LAMPINEN: My Data, My Terms: A Proposal for Personal Data Use Licenses. *Harvard Journal of Law & Technology*, vol. 33., Digest Spring 2020, https://jolt.law.harvard.edu/assets/digestImages/Paulius-Data-licenses-HJOLTDigest-Feb20.pdf. 9-11.

b. Az adatkezeléssel kapcsolatos szerepkörök a mesterséges intelligencia területén

Az újabb technológiai vívmányok révén, illetve az MI által végzett adatkezelések esetén sokszor jelentős kihívást jelent az adatkezeléssel kapcsolatos szerepkörök meghatározása, tekintettel arra, hogy az ilyen adatkezelések jellemzően nagy mennyiségű személyes adatot érintenek, kiterjedtek, sok esetben nehezen átláthatók, valamint sokszereplősek. A GDPR értelmében, a személyes adatok kezelése során adatkezelőnek az a személy vagy szervezet tekintendő, amely az adatkezelés céljait és eszközeit önállóan vagy másokkal együtt meghatározza,[278] míg adatfeldolgozónak tekintendő az a személy vagy szervezet, amely az adatkezelő nevében személyes adatokat kezel.[279] A GDPR külön rendelkezéseket tartalmaz továbbá a közös adatkezelőkre vonatkozóan is, amelyek az adatkezelés céljait és eszközeit közösen határozzák meg.[280] Így adatkezelőnek tekintendő például egy bank, amely a weboldalán a hatékonyabb ügyfélkiszolgálás érdekében egy chatbot alkalmazást működtet, és adatfeldolgozónak az az informatikai vállalkozás, amely a weboldal, illetve a chatbot kapcsán informatikai támogatást nyújt a bank részére. Ha a fenti chatbot alkalmazást, illetve a weboldalt több azonos cégcsoportba tartozó bank üzemelteti, amelyek például közösen tartanak fenn egy ügyfélkiszolgálást segítő weboldalt, úgy ennek kapcsán ezen bankok közös adatkezelőnek tekinthetők. Nem tekinthető azonban sem önálló, sem közös adatkezelőnek vagy adatfeldolgozónak a munkáltatója nevében eljáró munkavállaló, ennek adatkezeléssel járó tevékenysége ugyanis az őt alkalmazó adatkezelőnek tudható be.[281] Mindezen logika természetesen igaz például egy jogi értelemben vett személyiséggel nem rendelkező robot vagy szoftveres megoldás esetén is, abban az esetben is, ha az autonóm módon képes bizonyos kérdésekben dönteni, illetve bizonyos esetekben emberi felülvizsgálat nélkül működik.

Hangsúlyozandó továbbá, hogy más személy vagy szervezet nevében vagy érdekében, illetve megbízása alapján történő eljárás esetén a megbízott személy nem minden esetben tekinthető adatfeldolgozónak. Az adott szakmai szereplőket jelentős önálló jogosítványokkal felruházó, szabályozott szakmák esetén jellemzően az adott szereplő abban az esetben is önálló

[278] GDPR 4. cikk 7. pontja
[279] GDPR 4. cikk 8. pontja
[280] GDPR 26. cikk
[281] Lásd: ICO, What are 'controllers' and 'processors'?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#:~:text=Employees%20of%20the%20controller%20are,data%20on%20the%20controller's%20behalf.

adatkezelőnek tekinthető, ha a megbízója nevében jár el. Ilyennek tekinthetők például az ügyvédek vagy ügyvédi irodák is, tekintettel arra, hogy az ügyvédi megbízás jellemzően nem kizárólag az adatkezelésre, hanem eltérő feladatokra is kiterjed, az ügyvédi tevékenységet folytatók pedig viszonylagos önállóság mellett szervezik meg és végzik feladataikat a megbízójuk érdekében.[282] Így amennyiben egy ügyvédi iroda például egy ügyféllel szembeni hatósági eljárás kapcsán, a megbízás keretein belül nagyobb mennyiségű dokumentumok átvizsgálásához MI alapú kutatási rendszert alkalmaz (például: bizonyítékok könnyebb áttekintése, értékelése céljából), úgy ezen adatkezelés során jellemzően önálló adatkezelőként jár el. Emellett gyakorinak tekinthető, hogy például felhőszolgáltatást nyújtó vállalkozások MI megoldásokkal is támogatják ügyfeleiket (ideértve például egyes elemzési megoldásokat). A fenti esetekben, amennyiben az MI megoldás ezen kiegészítő, támogató funkciójához kapcsolódik az adatkezelés, úgy a felhőszolgáltató adatfeldolgozónak tekintendő, amennyiben azonban a személyes adatokat már a szolgáltatásai fejlesztéséhez vagy saját analitikai, marketing tevékenysége érdekében is felhasználja, úgy e körben adatkezelőnek tekintendő.[283]

A fenti szerepkörök azonban számos esetben csak nehezen különíthetők el MI-rendszerek alkalmazása esetén, egy adott személy vagy szervezet egymással szoros kapcsolatban álló adatkezelések esetén pedig akár több szerepkörben is megjelenhet. Például egy vállalatcsoport tagjainak közös rendszerüzemeltetése és támogatása esetén az egyes tagok megjelenhetnek a rendszeren tárolt ügyfél-, valamint munkavállalói adataik kapcsán adatkezelőként, figyelembe véve, hogy a saját munkavállalóikkal, valamint ügyfeleikkel az egyes tagok állnak szerződéses kapcsolatban; azonban egymás informatikai támogatása során megjelenhetnek a támogatott adatkezelői szervezet adatfeldolgozóiként is. Előfordulhat az is, hogy egyes adatkezelési műveleteket közös adatkezelőként végeznek a fentiek szerinti adatkezelők (például: az anyacég és a regionális központnak minősülő szervezetek), míg más adatkezelési műveleteket önállóan vagy a vállalatcsoport egy másik tagját támogató adatfeldolgozóként. Szintén közös adatkezelés valósulhat meg, amennyiben például két vállalkozás adatkészletének felhasználásával hoznak létre egy közös MI megoldást.[284] Vállalatcsoportok esetén továbbá az ebben résztvevő entitások az adattovábbítási stratégiájukat is adott esetben össze tudják hangolni, mindez az irányadó

[282] EDPB 07/2020. sz. iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról, 2.0 változat, elfogadva: 2021.07.07. („**07/2020. sz. Iránymutatás**"). 14.
[283] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Legal bases in data protection for the use of artificial intelligence, Discussion paper. Version 1.0, 2023.11.07, https://www.baden-wuerttemberg.datenschutz.de/legal-bases-in-data-protection-for-ai/ („**AI Discussion paper, Baden-Württemberg**") IV. 3.
[284] AI Discussion paper, Baden-Württemberg IV. 2.

követelmények elhanyagolását, de adott esetben hangsúlyosabb szabálykövetést is eredményezhet.[285]

Az MI Rendelet elsősorban az adott MI-rendszer vagy általános célú MI-modell szolgáltatójára helyezi a felelősséget, amely az adott rendszert vagy modellt fejleszti vagy kifejlesztette, és a saját neve vagy védjegye alatt forgalomba hozta vagy üzembe helyezte,[286] és ugyanezen felelősségi szabályokat alkalmazza – az irányadó szerződéses feltételekre tekintettel – a forgalmazóra, importőrre, alkalmazóra vagy egyéb harmadik félre is az adott magas kockázatú MI-rendszer sajátként történő megjelenítése, a rendszer, illetve rendeltetésének jelentős módosítása esetén.[287] A fenti szabályok alkalmazása hatással bírhat az adatkezeléssel kapcsolatos szerepek meghatározására is, amennyiben az adott MI-rendszert személyes adatok kezelésére használják. Így jellemzően az ilyen MI-rendszer szolgáltatója egyben az adatkezelés célját és eszközeit is meghatározza,[288] és így általában adatkezelőnek tekintendő, amennyiben azonban egy adott vállalkozás például egy másik vállalkozás által már korábban forgalomba hozott nagy kockázatú MI-rendszert a saját védjegyével vagy nevével lát el, az jellemzően az adatkezelés céljának, míg a rendszer jelentős módosítása adott esetben ezentúl az adatkezelés eszközének meghatározása kapcsán is értékelhető – mindez pedig az adatkezelői szerepek változásához is vezethet. Emellett előfordulhatnak olyan esetek is, ahol a szolgáltató vagy az alkalmazó más személy megbízásából működteti az adott MI-rendszert, és kezel ehhez kapcsolódóan személyes adatokat.[289] Mivel azonban az MI Rendelet a személyes és nem személyes adatokat kezelő MI-rendszerekre is vonatkozik, így értelemszerűen az MI Rendelet felelősségi szabályai önmagukban nem determinálják az adatkezeléssel kapcsolatos szerepeket, azok az adott eset körülményei tekintetében ítélhetők csak meg. Megjegyzendő továbbá, hogy az online térben jellemzően számos vállalkozás hozzáfér a felhasználók személyes adataihoz, amellyel elmosódhatnak az adatkezelői és adatfeldolgozói szerepek, valamint a hozzájuk kapcsolódó felelősség;[290] az MI alkalmazása pedig mindezt csak megkönnyíti, és felgyorsítja, ezért az MI-rendszerek révén személyes adatokat kezelőknek jellemzően még nagyobb

[285] KIS Kelemen Bence, HOHMAN Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikáció és jog*, 2016/2. 65.
[286] MI Rendelet 3. cikk 3. pontja
[287] MI Rendelet 25. cikk (1) bek.
[288] GDPR 4. cikk (7) bekezdés
[289] AEPD, Artificial Intelligence: Transparency, https://www.aepd.es/en/prensa-y-comunicacion/blog/artificial-intelligence-transparency
[290] TENE (2011) op. cit. 17.

figyelmet kell fordítaniuk adatkezelési szerepük egyértelmű meghatározására, valamint az átlátható adatkezelésre.

Hangsúlyozandó továbbá, hogy az adatkezeléssel kapcsolatos szerepek tükrében a feleknek megfelelő megállapodást kell kötniük egymással, amelynek – például MI-modell alkalmazása, implementálása esetén – ki kell terjednie a modellhez tartozó személyes adatok, illetve ilyen adatokat tartalmazó adatbázis felhasználására, az ezzel kapcsolatos adatvédelmi, adatbiztonsági követelményekre.[291] Erre tekintettel közös adatkezelők esetén ezeknek a közös adatkezeléssel kapcsolatos megállapodást szükséges kötniük, a megállapodás lényegét pedig szükséges összefoglalniuk, ezen összefoglalást pedig az érintettek rendelkezésére kell bocsátaniuk.[292] Így amennyiben két kutatóintézet közösen végez kutatást MI alapú megoldás alkalmazásával, úgy a résztvevőknek szóló adatvédelmi tájékoztatóban szükséges meghatározni a közös adatkezelőként eljáró szervezeteket, valamint ebben egyértelműen ismertetni szerepüket és az általuk végzett adatkezelési tevékenységet, az adatvédelmi követelményeknek való megfeleléssel kapcsolatos egyes releváns feladataikat (például: adatvédelmi hatásvizsgálat elvégzése, adatvédelmi incidensek kezelése, stb.). Ugyancsak, amennyiben egyik fél nem adatkezelőként, hanem adatfeldolgozóként támogatja a másik fél adatkezelési tevékenységét (például: a kutatást végző intézmény megbízása alapján MI alapú megoldást bocsát ezen intézmény rendelkezésére, amely az intézmény által meghatározott kutatás céljára használható), úgy az ennek megfelelő szerződést szükséges a feleknek megkötniük a GDPR-ban meghatározott tartalmi elemekkel.[293] A felek közti megállapodásnak az MI Rendelet hatálybalépésétől továbbá az MI Rendelet szerinti követelményeknek is adott esetben meg kell felelniük (különösen nagy kockázatú MI-rendszerek vagy általános célú MI megoldások esetén), így a megállapodásból egyértelműen következnie kell, hogy az adott MI-rendszer vagy modell kapcsán a felek milyen jogokkal, kötelezettségekkel, illetve felelősséggel bírnak, ideértve például az érintettek tájékoztatását a rendszer alkalmazása kapcsán. Mindez például az olyan szolgáltatók számára is jelentőséggel bírhat, amelyek például egy MI-modellt szolgáltatnak, amelyet azonban ténylegesen az ügyfelük implementál a saját környezetében, és használ fel a továbbiakban saját céljaira, a saját szolgáltatásai kapcsán.[294]

[291] AEPD, GDPR compliance of processings that embed Artificial Intelligence. An Introduction, February 2020, https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf ("**AEPD GDPR Compliance Introduction**"), 20.
[292] GDPR 26. cikk (2) bekezdés
[293] GDPR 28. cikk (3) bekezdés
[294] Bayerisches Landesamt für Datenschutzaufsicht („**BayLDA**"), Datenschutzkonforme Künstliche Intelligenz, Checkliste mit Prüfkriterien nach DS-GVO, 2024.01.24, https://www.lda.bayern.de/media/ki_checkliste.pdf

c. A mesterséges intelligencia és az átláthatóság

Az átláthatóság az egyik legalapvetőbb adatvédelmi követelménynek tekinthető, amely lehetővé teszi, hogy az érintettek tudomást szerezzenek személyes adataik kezeléséről, valamint erre tekintettel gyakorolhassák adatvédelmi jogaikat. Az átláthatóság biztosítása a fentiekre tekintettel az európai adatvédelmi jogban kiemelt jelentőséggel bír, így a GDPR-ban is az adatkezelő egyik alapvető kötelezettségeként, valamint alapelvként jelenik meg.[295] Ennek tükrében a személyes adatok kezelésével kapcsolatos, adatkezelő által nyújtott tájékoztatásnak, illetve kommunikációnak könnyen hozzáférhetőnek és közérthetőnek kell lennie, valamint az adatkezelőnek azokat világosan és egyszerű nyelvezettel szükséges megfogalmaznia,[296] hogy azt az érintettek megérthessék, és az adatkezelésre adott esetben ennek tükrében reagálhassanak (például személyes adataik törlését, illetve egyes adataikról való másolat kiadását kérve).

A fentiekre tekintettel elengedhetetlen, hogy az érintetteknek szóló adatvédelmi tájékoztató az érintettek által értett nyelven íródjon. Ez azonban túlmutat az érintett által beszélt nyelven való tájékoztatáson, szükséges ugyanis, hogy az érintettek ténylegesen megérthessék az adott tájékoztató szövegét. Átlag fogyasztók esetén például közismert, gyakran alkalmazott kifejezések, megfogalmazások alkalmazása ajánlott, míg szakszavak, kétértelmű vagy kevésbé ismert szófordulatok alkalmazása kerülendő. Erre a magyar adatvédelmi hatósági gyakorlatból jó példának tekinthető az „ügyfélszegmentáció" kifejezés használata, tekintettel arra, hogy ez a fogyasztók számára jellemzően nem érthető.[297] Szakértők, illetve egy adott területen jártas személyek részére szóló adatvédelmi tájékoztató esetén azonban alkalmazhatók az adott szakterületen alkalmazott, az adott személyek által jellemzően ismert szakkifejezések. Így például egy orvosi, kutatói személyzet számára szóló adatvédelmi tájékoztatóban használhatók orvosi szakkifejezések (például: egyes eljárások, vizsgálattípusok kapcsán történő adatkezelésekről való tájékoztatás), tekintettel arra, hogy ezt a tájékoztató címzettjei szakmájuk folytán feltehetőleg megértik.

A gyakorlatban azonban a különböző applikációk, weboldalak üzemeltetői, online szolgáltatások nyújtói jellemzően az adatkezelésekről csak általános leírást adó tájékoztatókat

[295] GDPR 5. cikk (1) a) pontja
[296] GDPR (39) preambulum-bekezdés
[297] NAIH/2015/2201/17/H. 30.

készítenek, amelyek az érintettek számára nehezen érthetők vagy semmitmondóak. Az adatvédelmi hatóságok azonban a gyakorlatban egyre jelentősebb figyelmet fordítanak az adatkezelési tájékoztatók megfelelőségére, valamint azok megfelelő értelmezhetőségére. A fentiek kapcsán például a svéd adatvédelmi hatóság 2023-ban 58 millió korona adatvédelmi bírságot szabott ki a Spotify nevű online zenei szolgáltatóval szemben, mivel a cég adatvédelmi tájékoztatója túlságosan általánosan fogalmazott, több esetben technikai szakszavakat használt, valamint kizárólag angolul volt elérhető, így azt a svéd felhasználók nem minden esetben érthették meg.[298] Magyarországon a közelmúltban a NAIH például a TV2 Média Csoport Zrt-vel szemben szabott ki bírságot, weboldalakon keresztüli átláthatatlan adatgyűjtés, elégtelen tájékoztatás miatt, ideértve az „*eszközön tárolt információk tárolása és/vagy elérése*" megfogalmazást, amelyet túlságosan tágnak tekintett.[299]

Az érintettek tájékoztatása kapcsán különös figyelmet érdemel a gyermekek megfelelő tájékoztatása személyes adataik kezeléséről, figyelembe véve, hogy az adatkezelés során a gyermekek személyes adatai különös védelmet érdemelnek, mindez pedig az adatkezelésről szóló tájékoztatás kapcsán is jelentőséggel bír. A gyermekek ugyanis életkoruknál fogva kevésbé képesek átlátni a személyes adataik megosztásával, kezelésével kapcsolatos kockázatokat, illetve következményeket, továbbá a rendelkezésükre álló lehetőségeket és jogokat.[300] Emellett a gyermekek jellemzően könnyebben befolyásolhatók mint felnőtt társaik, így a gyermekeket célzó egyes adatkezelések, különösen a marketing célú megkeresésekkel vagy egyes online szolgáltatásokkal, közösségi médiával kapcsolatos adatkezelési műveletek kapcsán kiemelten fontos az adatkezelés átláthatóságának biztosítása,[301] ideértve az adatkezelésről, valamint az érintetti jogokról való tájékoztatást is. Erre tekintettel az olyan adatkezelések vonatkozásában, amelyek kifejezetten gyermekekre vonatkoznak (például: játék applikációk), a tájékoztatást olyan nyelven szükséges megfogalmaznia az adatkezelőnek, amelyet az adott korosztályba tartozó gyermekek könnyen megérthetnek.[302] A nemzetközi gyakorlatból jó példának tekinthető az Egyesült Nemzetek Szervezetének („**ENSZ**") gyermekek jogairól szóló egyezményének gyermekbarát módon összefoglalt szövege, amely az

[298] Swedish Authority for Privacy Protection, Administrative fee against Spotify, 13 June 2023, https://www.imy.se/en/news/administrative-fee-against-spotify/
[299] NAIH-3195-11/2022. 4.2(ii). 16.
[300] GDPR (38) preambulum-bekezdés
[301] Uo.
[302] GDPR (58) preambulum-bekezdés

ENSZ weboldalán is elérhető.[303] Ennek kapcsán hangsúlyozandó, hogy a gyermekeknek szóló adatvédelmi tájékoztatókban halmozottan kerülni kell az olyan kifejezéseket, szófordulatokat, amelyek a közbeszédben nem számítanak elterjedtnek, és ezenfelül is olyan nyelvezet alkalmazandó, amelyet az érintett korosztályba tartozó gyermekek is megérthetnek (például: a komplex, elvont fogalmak helyett köznapi, egyszerű megfogalmazások). E körben több játékok gyártásával, forgalmazásával foglalkozó cég is publikált már gyermekek részére szóló adatvédelmi tájékoztatót, ideértve például a Lego vállalatot (amely egy adatkezeléseit, valamint az érintettek jogait gyermekek részére játékosan bemutató videót is közzétett a weboldalán).[304]

Megemlítendő továbbá, hogy a személyes adatok kezeléséről szóló, fentiek szerinti megfelelő tájékoztatást az adatkezelőnek a gyermek részére akkor is nyújtania kell, ha a gyermeket adott esetben törvényes képviselő vagy más személy képviseli (például: szülő, gondnok), ugyanis az adatkezelő tájékoztatási kötelezettsége nem hárítható át más személyre, a gyermek pedig, korára és értelmi képességeire tekintettel, jogosult a megfelelő tájékoztatásra személyes adatainak kezelésével kapcsolatban, ha az adatkezelés kifejezetten rá vonatkozik.[305] Természetesen azonban, ha a gyermek a fenti információk megértésére, befogadására fejlettségére, állapotára tekintettel nem képes (például: csecsemők esetén), úgy elegendő a nevükben eljáró személyek részére megadni a tájékoztatást, hiszen ilyen esetben a gyermek részére címzett tájékoztatás értelmetlen lenne vagy zavaróan hatna. A fentiek szerint, tehát, amennyiben egy gyermek egészségügyi adatait használják fel például egy egészségügyi MI alkalmazás fejlesztéséhez, és a gyermek részére megfelelő tájékoztatás nyújtható személyes adatai kezeléséről, úgy szükséges röviden a részére is összefoglalni az adatkezelés lényegét, így például, hogy az adatai gyűjtése és felhasználása miért szükséges az adott esetben, azok hogyan kerülnek felhasználásra. Ilyen esetben azonban az adatkezelőnek javasolt lehet mérlegelnie, hogy a tájékoztatás nem jár-e szükségtelen (például: pszichológiai vagy emocionális) megterheléssel a gyermek számára, különösen, ha adott esetben a nevében a törvényes képviselője jár el az adatkezelés kapcsán. Ilyen esetekben helyesebb lehet a tájékoztatást is

[303] Lásd: The Convention on the Rights of the Child: The child-friendly version, UNICEF https://www.unicef.org/sop/convention-rights-child-child-friendly-version, lásd továbbá az ezt hivatkozó Adatvédelmi Munkacsoport iránymutatásban: A 29. cikk szerinti munkacsoport, Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról, 17/HU, WP260 rev.01, elfogadás időpontja: 2017. november 29, a legutóbbi felülvizsgálat és elfogadás időpontja: 2018. április 11. ("**Átláthatósággal kapcsolatos Munkacsoport Vélemény**") 10.
[304] Lego, Now some serious stuff, https://www.lego.com/en-us/kids/legal/privacy-policy-short
[305] GDPR (58) preambulum-bekezdés

kizárólag a törvényes képviselőnek címezni az esetleges károk, a gyermekre nehezedő emocionális, illetve pszichológiai megterhelés elkerülése érdekében.

A tájékoztatással kapcsolatos egyes gyakorlati megoldások sok esetben a sérülékeny csoportokba tartozók egyéb személyek, például fogyatékkal élő vagy életkoruk, egészségügyi állapotuk okán más szövegezésű vagy eltérő formátumú információ befogadására képes személyek számára is segítséget nyújthatnak. Így a GDPR kifejezetten kiemeli annak lehetőségét, hogy az érintett tájékoztatása körében nyújtott információk szabványosított ikonokkal is kiegészítésre kerülhessenek, amelyeknek elektronikus környezetben géppel olvasható módon kell megjelenniük.[306] Emellett is lehetőség van továbbá a tájékoztatás és az azt segítő ikonok vizualizálására, például QR kódok vagy rövidebb tájékoztatóanyagok útján,[307] de akár az adatkezelés által indokoltak szerinti egyéb formátumban vagy módon is (például drónok által megfigyelt területen tábla kihelyezésével, illetve nyilvános tájékoztató kampányok útján).[308] E körben az adatkezelőt is különös felelősség terheli annak felismerése kapcsán, hogy az adatkezelése által érintett csoport vagy csoportok milyen jellemzőkkel bírnak, és ez a tájékoztatás milyen szövegezéssel, illetve milyen módon vagy formában való nyújtását teszi szükségessé. Egy látássérült érintetti csoport számára például megfelelőbb lehet a tájékoztatás szövegének online térben olyan módon való megjelenítése, amelyet a látássérülteket segítő programok is fel tudnak ismerni, illetve azt adott esetben például egy virtuális asszisztens is felolvashatja. A fizikai térben pedig jó megoldás lehet az ilyen érintetti csoport által látogatott helyen az adatvédelmi tájékoztatót Braille-írással is rendelkezésre bocsátani vagy szóban, illetve hangfelvétel segítségével is összefoglalni. Hangsúlyozandó, hogy egyes sérülékeny csoportba tartozó érintettek (például: kórházi betegek, idősotthonban ápolt személyek, látás-, illetve hallássérültek) vonatkozásában alkalmazott egészségügyi vagy szociális robotok esetén különösen jó megoldás lehet a robot általi rövid adatvédelmi tájékoztatás is (például: a robot által lejátszott hangfelvétel vagy képernyőn bemutatott videó), amelyet szükség esetén kiegészíthet az egészségügyi vagy szociális személyzet (például: kezelőorvos vagy ápolók) által adott további tájékoztatás, magyarázat is.

[306] GDPR 12. cikk (7) bek.
[307] Átláthatósággal kapcsolatos Munkacsoport Vélemény, 27-28.
[308] Átláthatósággal kapcsolatos Munkacsoport Vélemény, 24.

A Big Data-alapú, valamint az MI általi adatkezelésről adott tájékoztatás kapcsán gyakran merül fel a nehéz áttekinthetőség, megmagyarázhatóság problémája.[309] E körbe érthető az automatizált rendszerek által az internetről történő adatgyűjtés (angolul: „*web scraping*")[310] is. Ezen technikát gyakran használják MI-modellek tanítása során is. Igy például a népszerű, képgeneráló megoldások, mint például a Midjourney vagy a DALL-E is ezen a megközelítésen alapulnak. Az ilyen típusú adatkezelések felett az érintetteknek a gyakorlatban kevés hatalma van; ezek gyakran átláthatatlanok maradnak az érintettek számára, akik így nem is értesülhetnek arról, hogy az interneten nyilvánosan elérhető adataik, az általuk közzétett tartalmak felhasználásra kerülnek, például egy nagy nyelvi modell képzéséhez.

Emellett gyakori problémának tekinthető az MI által hozott döntések, kimenetek átláthatatlansága (ún. fekete doboz probléma). Az MI alkalmazása ugyanis adott esteben olyan eredményekhez is vezethet, amelyek előre nem láthatók, így sok esetben a személyes adatok kezelésének pontos hatásai, az ezek felhasználásával születő döntések és az ehhez vezető út sem térképezhetők fel teljes mértékben az adatkezelő által.[311] Megjegyzendő azonban, hogy a gyakorlatban már léteznek technológiai megoldások az MI általi döntéshozatallal kapcsolatos bizonytalanság kiküszöbölésére, a döntési folyamat kiszámíthatóságának növelésére. Ilyennek tekinthető például az IBM watsonx.governance elnevezésű megoldása, amelyet generatív, illetve gépi tanulási modellek értékelésére, nyomon követésére, pontosságának növelésére használnak.[312]

A fentiek kapcsán a GDPR is alapvető követelményként határozza meg az érintettek automatizált döntéshozatal, illetve a profilalkotás[313] tényéről való tájékoztatását, valamint azon információk rendelkezésre bocsátását, hogy az adatkezelés az érintettre nézve milyen jelentőséggel, illetve milyen várható következményekkel bír.[314] Így tehát az érintetteknek át

[309] ZŐDI (2017) i. m. 24.
[310] ICO, Generative AI first call for evidence: The lawful basis for web scraping to train generative AI models, https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-first-call-for-evidence
[311] Datatilsynet, Artificial intelligence and privacy, Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf
[312] IBM, watsonx.governance, https://www.ibm.com/products/watsonx-governance
[313] A GDPR 4. cikk 4. pontja értelmében profilalkotás: "*személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják*".
[314] GDPR 13. cikk (2) f) pontja, 14 cikk (2) g) pontja

kell látniuk az adatkezelés jelentőségét, helyzetükre, illetve jogaikra és szabadságaikra gyakorolt hatásait, azonban ez nem terjed ki szükségszerűen valamennyi lehetséges döntésre, kizárólag azok típusára, az érintettekre gyakorolt jellemző hatásokra, vonatkozó kockázatokra.

Mindez egyben segítséget is nyújt az érintett számára, hogy felmérhesse az MI általi adatkezelés jelentőségét és lehetséges hatásait, illetve – az érintett hozzájárulásán alapuló adatkezelés esetén – egyben az érintett döntéshozatalának is támaszul szolgálhat, míg emellett észszerű mértékű transzparencia megteremtését várja el az adatkezelőtől. Megemlítendő azonban, hogy az automatizált döntéshozatallal, valamint profilalkotással kapcsolatos megfelelő tájékoztatás nyújtása a fentiek tükrében gyakran kihívást jelenthet, ideértve azon eseteket, ahol az alkalmazott technológia, illetve az adatkezelési művelet különösen összetett, vagy ha az érintetti csoport sajátos tájékoztatási igényekkel bír, illetve szenzitívnek tekinthető.[315] Ilyen esetekben tehát az adatkezelőknek különös gondot kell fordítaniuk az adatkezelésről való megfelelő tájékoztatás nyújtására. Megemlítendő továbbá, hogy adott esetben az MI általi adatkezelésről való tájékoztatás lehetetlennek bizonyulhat vagy aránytalanul nagy erőfeszítést igényelhet az adatkezelő részéről. Ilyennek tekinthető adott esetben az MI fejlesztéséhez történő adatgyűjtés is az internetről vagy más nyilvános forrásokból, azonban jellemzően az érintetteknek ilyen esetekben is joguk lehet az arról való tájékoztatáshoz, hogy az adataikat MI fejlesztéshez és különböző szolgáltatásokhoz használják fel, az ilyen adatkezelést folytatóknak pedig nyilvánosan is számot kell adniuk az adatkezelésük jellemzőiről, ideértve az adatok forrását és az adatgyűjtés összefoglalását (különösen a jelentős adatéhséggel bíró nagy nyelvi modellek alkalmazása esetén).[316]

A gyakorlatban az automatizált döntéshozatal, illetve a profilalkotás kapcsán felmerülhet a kérdés, hogy az adatkezelő tájékoztatási kötelezettségének kizárólag a döntéshozatali mechanizmus mögötti logikára szükséges kiterjednie, vagy adott esetben a konkrét döntés magyarázatára is. E körben a Wachter, Mittelstadt és Floridi szerzőtriász amellett foglal állást,

[315] NECZ Dániel, Az adatkezelésről való tájékoztatás technológiai környezetben, különös tekintettel az Egyesült Államok szabályozására, *Jogi Fórum*, 2022.08.31. https://www.jogiforum.hu/wp-content/uploads/2022/09/necz-daniel_adatkezelesrol-valo-tajekoztatas-technologiai-kornyezetben_cimlappal.pdf [a továbbiakban: NECZ (2022a)]

[316] Philip HACKER, Andreas ENGEL, Marco MAUER: Regulating ChatGPT and other Large Generative AI Models. FAccT '23 Chicago (2023.06.12-15). arXiv:2302.02337v8, https://doi.org/10.48550/arXiv.2302.02337. 14.

miszerint az érintettnek a konkrét döntések megmagyarázásához nincsen joga,[317] ez ugyanis arra kötelezné az adatkezelőt, hogy jóslásokba bocsátkozzon az automatizált döntéshozatal érintettre gyakorolt hatásairól, ideértve adott esetben annak tisztázását is, hogy az adott döntést hogyan vehetik alapul más adatkezelők vagy adatfeldolgozók.[318] Ezzel szemben a Kim és Routledge szerzőpáros az adott automatizált döntéshozatali rendszer funkcionalitásával kapcsolatos ex-ante és ex-post, valamint az adott döntéssel kapcsolatos ex-post magyarázatot különböztetik meg,[319] leszögezik továbbá, hogy azon érintetteknek akik számára az automatizált döntéshozatal sérelemmel jár, rendelkezniük kell egyfajta joggal arra, hogy a rendszer funkcionalitásával kapcsolatos magyarázaton túl az adott döntés kapcsán is magyarázatot kapjanak („kárpótló tájékoztatás"), míg azon érintettek, akik számára az adott döntés nem jár sérelemmel, nem rendelkeznek ilyen joggal.[320] Az érintettek azonban tájékoztatást kell hogy kapjanak arról is, hogy az automatizált döntéshozatal további hatásokkal jár-e rájuk nézve; ezen tájékoztatásra („további tájékoztatás") az érintettek pedig akkor is jogosultak lehetnek, ha az adott megoldás, illetve döntés rájuk nézve nem sérelmes, ugyanis rájuk ilyenkor ettől függetlenül is hatással bírhat.[321] Ez utóbbi tájékoztatásra továbbá az érintettek akkor is jogosultak lehetnek, ha az adott megoldás általi döntés az érintettekre nem jár ugyan közvetlen hatással, azonban a személyes adataikat más adatkezelők érdekében dolgozzák fel.[322]

Akár a rendszer mögötti logikának, akár ennek és a konkrét döntésnek a megmagyarázhatóságából indulunk ki, leszögezendő azonban, hogy egy konkrét algoritmus megmagyarázhatóságához szükséges, hogy az adott algoritmus működése emberi nyelven is értelmezhető legyen, és egyértelmű legyen az érintettek számára, hogy az egyes algoritmus által értékelt tényezők hogyan hatnak ki az algoritmus által meghozott döntésekre.[323] Mindez azt is jelenti, hogy az adott MI-rendszert alkalmazónak tisztában kell lennie az adott rendszer mögötti

[317] Sandra WACHTER, Brent MITTELSTADT, Luciano FLORIDI: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, vol. 7., issue 2. (2017) 78.
[318] Wachter, Mittelstadt, Floridi op. cit. 83–84.
[319] Tae Wan KIM, Bryan R. ROUTLEDGE: Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach. *Business Ethics Quarterly*, vol. 32., no. 1 (2022). doi:10.1017/beq.2021.3. 80.
[320] KIM, ROUTLEDGE op. cit. 82.
[321] KIM, ROUTLEDGE op. cit. 90–91.
[322] KIM, ROUTLEDGE op. cit. 94–95.
[323] Bryce GOODMAN, Seth FLAXMAN: European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine*, vol. 38., no. 3. (2017), https://arxiv.org/abs/1606.08813v3, https://doi.org/10.48550/arXiv.1606.08813. 6.

logikai működéssel, valamint arról érthető módon szükséges tájékoztatnia az érintettet, a szükséges mértékben a rendszer döntéshozatalára befolyással bíró tényezők összefoglalásával.

A fentebb írtakat is figyelembe véve, álláspontunk szerint az adatkezelőnek az érintetteket az adott MI-rendszer mögötti alapvető logikáról, tehát a rendszer működéséről és annak hatásairól szükséges tájékoztatnia, amely kapcsán az adatkezelőnek a lehetőségeihez mérten könnyen érthető tájékoztatást szükséges nyújtania, a konkrét döntésekkel kapcsolatos magyarázathoz való jog pedig elsősorban azon esetekben illetheti meg az érintettet, ahol az MI alkalmazása az érintettre vonatkozó döntésekhez vezet, különösen ideértve a GDPR-ban meghatározottak szerint az érintettekre joghatással járó, vagy őket hasonlóan jelentős mértékben érintő döntéseket;[324] jellemzően ugyanis az ilyen döntések bírhatnak az érintettek életére a legjelentősebb hatással, az adatkezelőtől pedig elvárható, hogy az MI általi döntések hatásai és súlya szerinti tájékoztatást nyújtson. Az adatvédelem e körben jellemzően önmagában nem válaszolja meg azt, hogy az egyes döntésekhez – a GDPR-ban, illetve a fentebb ismertetetteken túl – pontosan milyen konkrét tájékoztatásnak kell kapcsolódnia, ezt ugyanis befolyásolja az adott tevékenység, a felek közti jogviszony és az irányadó egyéb jogszabályi rendelkezések alkalmazása is (például: munkáltató általi döntések esetén ezek esetleges indokolása a munkajogi jogszabályi követelményekkel összhangban történhet).

Hangsúlyozandó, hogy az MI Rendelet maga is jogot biztosít az egyéni döntéshozatal magyarázatához valamennyi olyan nagy kockázatú MI rendszerek által érintett személy számára, aki olyan döntés hatálya alá tartozik, amely joghatásokat vált ki, vagy őt hasonlóan jelentősen érinti oly módon, hogy hogy annak megítélése szerint a döntés kedvezőtlen hatást gyakorol az egészségére, biztonságára vagy alapvető jogaira. Ezen esetekben az érintett jogosult arra, hogy egyértelmű és érdemi magyarázatot kapjon az MI-rendszer döntéshozatali eljárásban betöltött szerepéről és a hozott döntés fő elemeiről.[325] Ezen rendelkezések azonban nem alkalmazandók a kritikus digitális infrastruktúra biztonsági alkotórészeként való használatra szánt MI-rendszerekre, valamint az olyan, fenti kötelezettség alóli kivételek esetén, amelyek az uniós jogból vagy az annak megfelelő nemzeti jogból következnek[326] (ilyenek minősülhet például a nemzetbiztonsági szolgálatok vagy bűnüldöző hatóságok által alkalmazott egyes rendszerek használata), illetve a megmagyarázhatósághoz való jog is csak annyiban

[324] GDPR 22. cikk (1) bekezdés
[325] MI Rendelet 86. cikk (1) bek.
[326] MI Rendelet 86. cikk (2) bek.

gyakorolható, amennyiben az uniós jog az említett jogról másként nem rendelkezik.[327] Ez utóbbi esetben kérdéses, hogy a GDPR a gyakorlatban mekkora „teret engednek" majd az MI Rendelet szerinti megmagyarázhatósághoz való jog érvényesülésének a GDPR tájékoztatáshoz való joggal kapcsolatos rendelkezései olyan esetekben ahol az adott MI-rendszert személyes adatok kezelésére használják, illetve hogyan is értelmezik majd az adatvédelmi hatóságok, illetve a bíróságok ilyen helyzetekben a fenti két átláthatósággal kapcsolatos jog viszonyát.

Az MI-rendszerek általi adatkezelés kapcsán megjegyzendő továbbá, hogy az adatvédelmi hatósági gyakorlat is egyre nagyobb figyelmet fordít az automatizált döntéshozatalra, illetve a profilalkotásra, valamint az MI-rendszerek révén végzett átlátható adatkezelésre. Berlin Adatvédelmi és Információszabadsági Biztosa például 2023-ban egy bank automatizált hitelbírálattal kapcsolatos adatkezelése kapcsán állapított meg jogsértést, valamint szabott ki 300.000 euró összegű bírságot, tekintettel arra, hogy a fenti adatkezelés az ügyfelek irányában átláthatatlan módon történt, így az ügyfelek nem kaphattak megfelelő tájékoztatást a hitelkérelmeik automatizált döntéshozatal útján való elutasításának alapjáról sem.[328]

A fentiek kapcsán szintén jelentős kihívást jelentenek az online térben adatvédelmi szempontból az úgynevezett „sötét minták", amelyek jellemzően olyan kialakítások, például weboldalakon vagy applikációkon, illetve olyan szolgáltatói gyakorlatok, amelyek a felhasználókat akaratuk ellenére, sok esetben a részükre hátrányos döntések meghozatalára kényszerítik, vagy az akaratukat ilyen megoldások révén hajlítják (például: bizonyos információk elhallgatásával vagy kiemelésével).[329] A sötét megoldások többféle szempont alapján csoportosíthatók, illetve többféle kategóriába sorolhatók. Az EDPB meghatározása szerint a sötét megoldások az alábbi kategóriákba sorolhatók:

- Túlterhelés („*overloading*"): az érintettek kérelmekkel, információval való elárasztása;
- Átugrás („*skipping*"): olyan megoldás alkalmazása, amelynek révén az érintett figyelmen kívül hagyja (mintegy „átugorja") az adatvédelmi szempontokot, illetve az adott felület ezen szempontból releváns részeit;
- Felkavarás („*stirring*"): az érintett döntésének befolyásolása, elsősorban az érintett érzelmeire, ingereire való hatás révén;

[327] MI Rendelet 86. cikk (3) bek.
[328] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Computer sagt Nein, 2023.05.31, https://www.datenschutz-berlin.de/pressemitteilung/computer-sagt-nein/
[329] Az EDPB 3/2022. számú iránymutatása a sötét megoldásokról a közösségi média platformok felületein: hogyan ismerhetők fel és kerülhetők el, 1. verzió, 2022.03.14 („**EDPB 3/2022. sz. Iránymutatása**") 2.

- Akadályozás („*hindering*”): az érintett tájékoztatását vagy adatvédelmi jogainak gyakorlását akadályozó megoldások;
- Összezavarás („*fickle*”): nehezen áttekinthető vagy össze nem függő felület és tájékoztatás kialakítása az érintett megtévesztése, valamint adatvédelmi jogai gyakorlásának megnehezítése érdekében;
- Egyedül hagyás („*left in the dark*”): bizonyos információkat, illetve az adatvédelmi jogok gyakorlására szolgáló megoldásokat elhallgató, az érintettet bizonytalanságban tartó kialakítás.[330]

A fentebb írtak jelenségek természetesen az adott eset körülményeire tekintettel értelmezendők, tekintettel arra, hogy e körben az EDPB általános tilalmak felállítását nem célozta,[331] kizárólag a transzparens adatkezelési gyakorlat kialakításának segítését. Emellett a sötét megoldások természetesen egyéb szempontok szerint is csoportosíthatók, az egyes kategóriákon belül pedig további alkategóriák képezhetők, illetve további típusok határozhatók meg. A Horváth Anna Zsófia és Domokos Márton szerzőpáros például a sötét megoldásokat két csoportba sorolja: 1) a felhasználó számára elérhető információt, illetve információáramlást befolyásoló, valamint 2) a felhasználó döntési folyamatát befolyásoló megoldásokat.[332] Maga az EDPB 3/2022. sz. Iránymutatása pedig a fenti kategóriákon belül különböző alkategóriákat képez. Így például a felhasználók „egyedül hagyásának” („*left in the dark*”) kategóriáján belül a nyelvi következetlenség („*language discontinuity*”), az ellentmondásos információk („*conflicting information*”), valamint a kétértelmű kifejezések és információk („*ambiguous wording or information*”) alkategóriákat különbözteti meg.[333] A sötét minták sajnálatosan napjainkban az online szolgáltatások kapcsán gyakorinak tekinthetők, az MI segítségével pedig még hatékonyabban képesek a felhasználók manipulálására, valamint viselkedésükkel kapcsolatos információk kinyerésére és további elemzésére. A YouTube például 18 év feletti felhasználók esetén az „Autoplay” funkciót alapbeállításként alkalmazza,[334] így a YouTube egymás után képes lejátszani a korábbihoz hasonló, illetve a felhasználó érdeklődési körébe eső

[330] EDPB 3/2022. sz. Iránymutatása, 7-8.
[331] PUSZTAHELYI Réka: A személyes adatok üzleti célú megszerzésére alkalmazott „sötét minták” elleni fellépés lehetséges formái. *In Medias Res*, 2023/2. 163.
[332] DOMOKOS Márton, HORVÁTH Anna Zsófia: Dark patterns – napvilágra kerülő sötét megoldások. *Jogi Fórum*, 2021.09.02. https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/
[333] EDPB 3/2022. sz. Iránymutatása, 63-64.
[334] YouTube Help. Autoplay videos, https://support.google.com/youtube/answer/6327615?hl=en#:~:text=If%20you're%2018%20or,Autoplay%20settings%20for%20different%20devices

videótartalmakat, így még inkább lekötve a felhasználók figyelmét,[335] egyúttal lehetővé téve adataik hatékonyabb kiaknázását.

Természetesen az érintett tájékoztatása tekintetében a tájékoztatás időpontjának is különös jelentősége van, a nem megfelelő időpontban nyújtott tájékoztatás ugyanis az érintettet bizonytalanságban tarthatja, illetve adatvédelmi jogai gyakorlásának aránytalan korlátozásához vezethet. A GDPR ennek kapcsán kiemeli, miszerint az adatok érintettől való gyűjtése esetén a tájékoztatást az adatkezelőnek a személyes adatok megszerzésének időpontjában szükséges nyújtania.[336] Amennyiben pedig az adatokat más forrásból szerezték, úgy a tájékoztatást az adatkezelés körülményeire tekintettel, észszerű határidőn, de legkésőbb egy hónapon belül szükséges megadni; az érintettel való kapcsolattartás céljára felhasznált adatok kezelése esetén azonban legkésőbb az első kapcsolatfelvételkor, míg ha várhatóan más címzettel is közlik a személyes adatokat, úgy az első alkalommal való közléskor.[337] A fentiekre tekintettel például egy chatbot alkalmazása esetén jó megoldás lehet a chatbot alkalmazás megnyitásakor, esetleges új funkciók elindításakor, illetve az érintett kérésére megjeleníteni az adatvédelmi tájékoztató elérhetőségét, amelynek egyes releváns rendelkezéseit – például az érintett kérdésére válaszként – a chatbot külön is megjelenítheti. Megemlítendő továbbá, hogy a kapcsolattartási adatok kezelése számos esetben különös jelentőséggel bírhat, és lehetőséget teremthet az egyedi adatokon túlmutatóan az érintett kapcsolataira és szokásaira is, így ilyen esetekben (például: az érintett közösségi média profiljának, kapcsolati hálójának kezelése esetén) az érintett adatkör a személyes adatok védelmén túl a magánszférához való joggal és az emberi méltósághoz való joggal is szoros kapcsolatban állhat.[338]

A tájékoztatás kötelezettsége alól azonban kivételek is meghatározhatók, ideértve különösen azon eseteket, amikor az érintett már rendelkezik a tájékoztatás körébe tartozó információkkal.[339] Így tehát, amennyiben az érintett már korábban tudomást szerzett arról, hogy személyes adatait MI-rendszer alkalmazásával kezelik (például: az adott felhasználó már korábban is tájékoztatást kapott arról, hogy a chatbot részére megadott információi hogyan kerülnek felhasználásra), úgy ennek kapcsán a körülmények változatlansága esetén

[335] Katherine MILLER: Can't Unsubscribe? Blame Dark Patterns. *Stanford University, Human-Centered Artificial Intelligence*, 2021.12.13, https://hai.stanford.edu/news/cant-unsubscribe-blame-dark-patterns
[336] GDPR 13. cikk (1) bek.
[337] GDPR 14. cikk (3) bek.
[338] 15/2022. (VII. 14.) AB határozat. [20].
[339] GDPR 13. cikk (4) bek., GDPR 14. cikk (5) bek. a) pontja

szükségtelen az érintettet (újból) tájékoztatni. Mivel azonban ez jellemzően nagyobb nehézséggel nem jár az adatkezelő számára, így ilyen esetekben is jó gyakorlat lehet, ha például a chatbot felhasználói kérésre az adatvédelmi tájékoztatót vagy annak vonatkozó részeit megjeleníti, így segítve a felhasználó könnyebb eligazodását, az adatkezelés áttekintését, adatvédelmi jogai megismerését.

Emellett, ha a személyes adatokat nem az érintettől gyűjtik, további kivételt jelenthet, ha adott helyzetben a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyulna vagy aránytalanul nagy erőfeszítést igényelne, e körbe értve különösen a közérdekű archiválás céljából végzett, a történelmi és kutatási, illetve statisztikai célú adatkezelést.[340] Amennyiben tehát történelmi kutatás céljából MI megoldás alkalmazásával végzik évtizedekkel ezelőtti újságcikkek és tanulmányok elemzését, nem várható el észszerűen a kutatást végzőktől az ezen dokumentumokban említett valamennyi személy felkeresése és tájékoztatása. Szintén kivételt jelent az irányadó uniós vagy tagállami jog által előírt adatgyűjtéssel, illetve közléssel kapcsolatban történő tájékoztatás adása (tekintettel arra, hogy az érintett erre jellemzően számíthat, és az adatkezelő is kötelezően végzi az adatkezelést), valamint az uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettségnek megfelelő adatkezelés.[341] Így például, adott esetben hivatkozhat egy ügyvédi iroda is ezen kivételre, amennyiben az ügyfele megbízásából MI-alapú megoldással keres bizonyítékokat e-mailek és más dokumentumok között, tekintettel arra, hogy az ezen e-mailekben vagy dokumentumokban említett érintettek tájékoztatása a megbízó érdekei ellen hathat, illetve ügyvédi titok felfedéséhez vezethet.

d. A mesterséges intelligencia általi adatkezelés jogszerűsége

Az MI általi adatkezelés jogszerűsége a megbízható MI alkalmazása szempontjából kiemelt jelentőséggel bír. Az MI szabályozásával kapcsolatos alapelveket, valamint a technológia alkalmazásával kapcsolatos etikai szempontokat a tanulmány korábbi fejezetében már tárgyaltuk,[342] így az alábbiakban kifejezetten az MI általi adatkezelés jogszerűségére, valamint a megfelelő jogalapok hivatkozására fókuszálunk.

[340] GDPR 14. cikk (5) bek. b) pontja
[341] GDPR 14. cikk (5) bek. c-d) pontjai
[342] Lásd: a tanulmány mesterséges intelligencia szabályozásával kapcsolatos fejezetét.

Az adatkezelés jogszerűsége kapcsán az EU-n belül kiemelt jelentőséggel bír a GDPR-ban meghatározott, személyes adatok kezelésére vonatkozó alapelveknek történő megfelelés, ideértve a személyes adatok

- jogszerű és tisztességes, valamint az érintett számára átlátható módon történő kezelését („jogszerűség, tisztességes eljárás és átláthatóság”),
- meghatározott, egyértelmű és jogszerű célból történő gyűjtését, valamint ezen célokkal összeegyeztethető módon való kezelését („célhoz kötöttség”),
- adatkezelés céljai szempontjából való megfelelőségét és releváns mivoltát, valamint kezelésük szükséges mértékűre való korlátozását („adattakarékosság”),
- pontosságát és szükség esetén naprakészségét („pontosság”),
- olyan formában történő tárolását, amely az érintettek azonosítását csak az adatkezelés céljainak eléréséhez szükséges ideig teszi lehetővé („korlátozott tárolhatóság”),
- olyan módon való kezelését, amely révén megfelelő technikai és szervezési intézkedésekkel biztosításra kerül a személyes adatok megfelelő biztonsága („integritás és bizalmas jelleg”).[343]

A fentiek mellett a GDPR kiemeli, miszerint az adatkezelő felelős a fenti alapelveknek való megfelelésért, valamint képesnek kell lennie a megfelelés igazolására („elszámoltathatóság”),[344] így utolsó alapelvként szerepeltetve az alapelveknek való megfelelő adatkezelést és annak szükség szerinti igazolását.

A fenti alapelveknek – amennyiben az adott MI-rendszer alkalmazása esetén személyes adatok kezelésére is sor kerül – a GDPR szabályai szerint az MI általi adatkezelés kapcsán is érvényesülniük kell. Ezen alapelvek azonban a gyakorlatban több szempontból is sajátosan vagy kérdésesen foghatnak helyt az MI általi adatkezelés kapcsán. Így például sajátosan, illetve csak bizonyos részben értelmezhető a jogszerű és tisztességes eljárás és átláthatóság alapelvi követelménye, mivel az MI általi adatkezelés folyamata sok esetben átláthatatlan, az MI által levont bizonyos következtetések, döntések és az ehhez vezető logikai folyamat kapcsán az adott megoldás szolgáltatója sem képes feltétlenül teljeskörű magyarázatot nyújtani. Tekintettel arra, hogy a jogszerűség, tisztességes eljárás és átláthatóság alapelveinek egymásra tekintettel,

[343] GDPR 5. cikk (1) bek.
[344] GDPR 5. cikk (2) bek.

egyszerre kell érvényesülniük a GDPR alatt,[345] így az MI megoldásokat alkalmazó adatkezelőtől ezen alapelv szerint elvárható különösen az adatkezeléssel járó kockázatok előzetes felmérése (különös adatvédelmi hatásvizsgálat keretében), azok kiküszöbölésére vagy csökkentésére szolgáló megfelelő intézkedések alkalmazása, valamint az érintettek ezzel kapcsolatos tájékoztatása annak érdekében, hogy az adatkezelésre és annak hatásaira, esetleges kockázataira megfelelően felkészülhessenek.[346] Az átláthatóság és a tisztességes eljárás ilyen kockázat-alapú, az adatkezelés lényegére fókuszáló biztosítása – különösen az egyes specifikus feladatok ellátására kifejlesztette MI-rendszerek esetén – adott esetben praktikusabb módon lenne garantálható mint az adatkezelés részleteibe menő tájékoztatás. Az általános célú vagy a jellemzően több funkcióval rendelkező, az internetről, illetve nyilvános adatbázisokból adatokat gyűjtő MI-rendszerek kapcsán azonban már problémás lehet akár a fenti „szűkebb értelemben vett átláthatóság" biztosítása is. Például egy ChatGPT-hez hasonló, a nyilvános interneten is kereső multimodális megoldás esetén hogyan garantálható a felhasználókon kívüli érintettek tájékoztatása? Elégséges-e az adott szolgáltató weboldalán ezzel kapcsolatos tájékoztatás elhelyezése, vagy további lépések megtétele is szükséges (például: az adott megoldással kapcsolatos szélesebb körű nyilvános tájékoztatás)? Ezekre a kérdésekre ma még nehéz egyértelmű választ adni.

Szintén kulcsfontosságúnak tekintendő az adatkezelés célhoz kötöttségének alapelve, amelynek keretében az adatkezelő nem csak saját érdekeit, hanem az érintett pozícióját is értékeli, és erre tekintettel határozza meg az adott cél eléréséhez szükséges adatkört, valamint szervezi meg az adatkezelést.[347] Az eredeti céllal összeegyeztethetőnek minősíti továbbá a GDPR közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelést,[348] nem zárja ki azonban adott esetben egyéb, az eredeti céllal összeegyeztethető adatkezelések lehetőségét. A célhoz kötöttség elvének történő megfelelés azonban az MI általi adatkezelés esetén a gyakorlatban kihívásokba ütközhet, ugyanis az MI-rendszerek, különösen az általános célú MI-rendszerek jellemzően többféle célból kezelnek személyes adatokat, az adatkezelés egyes céljai pedig sokszor csak a későbbiekben alakulnak

[345] ESZTERI Dániel: Elosztott mesterséges intelligencia fejlesztés blokklánc alapon az adatvédelem érvényesülése érdekében. *Pro Futuro*, 2020/1. https://doi.org/10.26521/Profuturo/2020/1/7554. 20.
[346] NECZ Dániel: A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai. *Acta Humana – Emberi Jogi Közlemények*, 2022/3. https://doi.org/10.32566/ah.2022.3.4. 101. [a továbbiakban: NECZ (2022b)]
[347] RÉVÉSZ Balázs, Az adatkezelés alapelvei. In: PÉTERFALVI Attila, RÉVÉSZ Balázs, BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary Kft., 2021. 105.
[348] GDPR 5. cikk (1) bek. b) pontja

ki vagy válnak világossá, így azok kapcsán az érintettek előzetes tájékoztatására sincs értelemszerű lehetőség. A gyakorlat ugyanakkor vélhetően ezen kérdésben az MI-alapú megoldások elterjedésével engedékenyebb lesz. A francia adatvédelmi hatóság például az MI általi adatkezeléssel kapcsolatos tájékoztatóanyagában akként foglalt állást, hogy például egy videómegosztó-platform esetén adott esetben a felhasználói előzményeknek a szolgáltatás személyre szabása érdekében való felhasználása is minősülhet az eredeti céllal összeférhetőnek, amelyhez nem szükséges az érintett előzetes hozzájárulása, azonban a szolgáltatónak biztosítania kell az érintett tiltakozáshoz való jogát.[349]

Az adatkezelés kapcsán kiemelt fontossággal bírnak továbbá az adattakarékosságra, az adatkezelés pontosságára, valamint a korlátozott tárolhatóságra vonatkozó alapelvek, amelyek értelmében kizárólag az adatkezelési cél eléréséhez szükséges, naprakész és pontos személyes adatok kezelhetők, az érintetteket az adatkezelési cél elérésének tükrében, a szükséges ideig és módon azonosítva. Erre tekintettel a fenti alapelveknek történő megfelelés érdekében az adatkezelés egyes szakaszait is akként lenne szükséges meghatározniuk az MI általi adatkezelést folytatóknak, hogy az érintettek csak a szükséges ideig maradjanak azonosíthatók, míg az adatkezelés későbbi vagy egyéb szakaszaiban az adatkezelés anonimizált (például: statisztikai adatok) módon végezhető.

Belátható azonban, hogy ezen statikusnak tekinthető fenti megközelítés jellemzően nem garantálható az adatgazdaság korában. A technológiai nagyvállalatok számos, publikus és privát forrásból gyűjtenek, szinte beláthatatlan mennyiségű személyes adatok, amelyeket eltérő célokból használnak fel; így – ahogy Omer Tene és Jules Polonetsky is kiemelik – napjainkra az adatminimalizálás a gyakorlatban már csak kérdésesen tekinthető alapkövetelménynek, ezen folyamatot pedig az MI csak felgyorsítja, így inkább az adott adatkezelés hasznosságát kellene összevetni annak hátrányaival, mintsem a fenti alapelvhez való feltétlen ragaszkodást megkövetelni.[350] Emellett az MI alkalmazása is számos esetben megköveteli az érintett azonosíthatóságának fenntartását (például: közszereplőkre vonatkozó információk kezelése egy chatbot által, vagy ha az érintett adatainak kezelése a szolgáltatás elvégzéséhez, annak személyre szabottan történő nyújtásához szükséges), valamint az MI adott esetben – a

[349] CNIL, AI how-to sheets. Ensuring the lawfulness of the data processing, https://cnil.fr/en/ensuring-lawfulness-data-processing ("**CNIL AI how-to sheets**").
[350] Omer TENE, Jules POLONETSKY: Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, vol. 11., issue 5. (2013) 260.

vonatkozó adatkörre és az adatkezelés egyéb körülményeire tekintettel – képes lehet akár anonimizált adatok alapján is, például azok összevetésével, konkrét személyeket azonosítani. Megjegyzendő továbbá, hogy bár a kezelt adatok naprakészsége az MI általi adatkezelés esetén is jellemzően fontos szempontot képez, nem garantálható valamennyi esetben, ugyanis a hibás vagy pontatlan adatok megőrzésére is szükség lehet az esetleges hibás működés felfedéséhez és kijavításához.[351] A fentieken túl továbbá az MI általi adatkezelést végzőknek az integritás és bizalmas jelleg elvéből kiindulva a személyes adatokat megfelelő védelem és titoktartás mellett kell kezelniük, amely egyben az illetéktelenek általi hozzáférhetőséget is kizárja. Ezen követelmény teljesítése különös kihívást jelenthet a különböző chatbot alkalmazások vagy generatív MI-rendszerek esetén, amelyek a tanulási folyamat során jellemzően a felhasználók által betáplált információkat, megosztott tartalmakat is alapul veszik, így akarva-akaratlanul a későbbi eredmények során, más felhasználóknál is felbukkanhatnak.[352]

Természetesen az MI általi adatkezelés esetén a fenti elveknek való megfelelésen túl szükséges a megfelelő jogalap kiválasztása is.[353] A GDPR mint az EU kiemelkedő adatvédelmi jogszabálya hat jogalapot határoz meg, amelyek alapján a személyes adatok kezelhetők, ideértve

- a hozzájárulást,
- az érintettel közvetlenül kötött szerződést és az azt megelőző, érintett kérésére eszközölt lépéseket,
- az adatkezelőre irányadó jogi kötelezettség teljesítését,
- az érintett vagy másik természetes személy létfontosságú érdekeit,
- a közérdeket vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlását,
- az adatkezelő vagy harmadik fél jogos érdekét.[354]

A személyes adatok kezelése tehát az EU-n belül a fenti jogalapok valamelyikére támaszkodva történhet, amely az MI általi adatkezelések esetén is irányadó. Az adatkezelés egyik igen

[351] NECZ (2022b). i. m. 102–103.
[352] Lance ELIOT: Generative AI ChatGPT Can Disturbingly Gobble Up Your Private And Confidential Data, Forewarns AI Ethics And AI Law, *Forbes*, 2023.01.27. https://www.forbes.com/sites/lanceeliot/2023/01/27/generative-ai-chatgpt-can-disturbingly-gobble-up-your-private-and-confidential-data-forewarns-ai-ethics-and-ai-law/
[353] Az adatkezelés alapelveinek történő megfelelést és a helyes jogalap megválasztását annak szoros összefüggéseire tekintettel más műveinkben is jellemzően egy fejezetben tárgyaltuk. Lásd: Necz (2022b). i. m. 100–106, Necz (2020a). i. m. 142–150.
[354] GDPR 6. cikk

gyakran idézett jogalapjaként a hozzájárulás[355] tekinthető, amelynek megfelelő hivatkozása esetén azonban több feltételnek is teljesülnie kell. Így a hozzájárulásnak a) önkéntesnek, b) konkrétnak, c) tájékoztatáson alapulónak és d) egyértelműnek kell lennie.[356] A fenti feltételek bármelyikének hiányában a hozzájárulás nem tekinthető megfelelőnek, és ha erre lehetőség van, a hozzájárulás helyett az adatkezelés eltérő jogalapra helyezendő. Tekintettel azonban arra, hogy a fenti feltétek megléte a gyakorlatban sok esetben vitatható, illetve kérdésesnek tekinthető, így azokat érdemes külön-külön is megvizsgálni, különösen az MI általi adatkezelés kontextusában.

A fentiekre tekintettel a hozzájárulás önkéntességéhez az érintett szabad választásának lehetősége szükséges,[357] amelyet jellemzően kizár, többek között, az egyenlőtlen viszonyban, kényszer vagy szankciótól való félelem hatására adott hozzájárulás, illetve a szükségtelenül összekapcsolt vagy szerződéskötés, szolgáltatás igénybevétele által megkövetelt hozzájárulás megadása.[358] Ilyen esetekben ugyanis az érintett nincs abban a helyzetben, hogy szabadon, külső befolyás nélkül hozhasson döntést a hozzájárulás megadásáról. Erre jó példának tekinthető általában a munkaviszonyban adott hozzájárulás. Amennyiben például az MI alapú megoldás általi megfigyelést a munkáltató a munkavállaló hozzájárulása alapján kívánja végezni a munkahelyen (például: arcfelismerést végző vagy egyéb biztonsági rendszer alapján), úgy a hozzájárulás nem lesz megfelelő jogalap, mivel valószínűleg ehhez a munkáltatói szankciótól való félelem hiányában a munkavállalók nem járulnának hozzá önkéntesen.[359] Emellett az online térben is gyakran merül fel a kérdés, miszerint a hozzájárulást az érintett valóban önkéntesen adta-e egy bizonyos applikáció vagy weboldal használata, szolgáltatás igénybevétele során. Amennyiben ugyanis az érintett nem adja hozzájárulását az adott adatkezeléshez (például: nem regisztrál a szolgáltatásra), úgy kevesebb esélye lehet arra, hogy ismerőseivel vagy más személyekkel kapcsolatba lépjen, így a hozzájárulás az adott körülmények tükrében kikényszerítetté válik.[360]

A fentiekre tekintettel tehát a hozzájárulásnak nem csak önkéntesnek, hanem konkrétnak és egyértelműnek is kell lennie. Így a hozzájárulásnak konkrét és meghatározott adatkezelésre

[355] GDPR 6. cikk (1) a) pontja
[356] GDPR (32) preambulum-bekezdése
[357] GDPR (42) preambulum-bekezdése
[358] GDPR (43) preambulum-bekezdése
[359] Lásd: NAIH/2020/2729/15. 10. sz. ügyben hozott határozat
[360] Adam J. ANDREOTTA, Nin KIRKHAM, Marco RIZZI: AI, big data, and the future of consent. *AI & Society*, vol. 37. (2022), https://doi.org/10.1007/s00146-021-01262-5. 1721.

szükséges felhatalmazást adnia, valamint abból egyértelműen következnie kell az adatkezelő számára az érintett akaratának, egyben az adatkezelés hozzájárulás által megadott terjedelmének. E körben jelentős különbség van a között, ha az érintett az MI által kezelt adatokat saját maga adja meg, vagy ha az érintettre vonatkozó információkat az MI más forrásból gyűjti, illetve, ha más kezdeményezésére történik az adatkezelés. Így például, ha a chatbot-ot alkalmazó felhasználó a prompt-ban saját magára vonatkozó információkat ad meg az adatkezeléshez (például: egy e-mail átfogalmazása vagy egy önéletrajz szerkesztése érdekében), úgy ez adott esetben tekinthető az érintett önkéntes hozzájárulásának a vonatkozó adatkezeléshez.[361] A hozzájárulás azonban értelemszerűen nem szolgálhat jogalapul, ha a felhasználó harmadik személy adatait adja meg (például: az átfogalmazandó e-mail szövegében említett, felhasználón kívüli személyek), tekintettel arra, hogy ezen személyek jellemzően nem az adott MI alkalmazás felhasználói, illetve az az általi adatkezelésről nem, vagy csak korlátozott információkkal bírhatnak.[362]

Hangsúlyozandó továbbá, hogy napjainkban számos online platform, illetve webáruház használ algoritmusokat szolgáltatásaik fejlesztése, vásárlási ajánlataik optimalizálása érdekében (például: egyes fogyasztói csoportok jellemzőinek, adott fogyasztó vásárlási előzményeinek figyelembevételével). Amennyiben a szolgáltató az érintett hozzájárulása alapján folytat a fentiek szerinti adatkezelést, úgy az érintett előzetes tájékoztatása különös jelentőséggel bír, kérdéses ugyanis, hogy az érintett ilyen esetekben megfelelő tájékoztatás hiányában mennyire számíthat arra, hogy egyes jellemzőit, vásárlási előzményeit algoritmusok elemezzék, és ez alapján küldjenek a részére őt valószínűleg érdeklő vagy számára adott esetben hasznos ajánlatokat, kedvezményeket.[363] Ennek kapcsán kiemelendő az EUB IAB elnevezésű európai reklámszervezet hozzájárulás-kezelési mechanizmusával kapcsolatos ügye. Ennek kapcsán az IAB Europe „*Transparency & Consent Framework*" elnevezésű, online marketing célú adatkezeléssel kapcsolatos keretrendszerét[364] a belga adatvédelmi hatóság 2022-ben

[361] Claudio NOVELLI, Federico CASOLARI, Philipp HACKER, Giorgio SPEDICATO, Luciano FLORIDI: *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity*. 2024.01.17, last revised: 2024.03.15.), arXiv:2401.07348v4, https://doi.org/10.48550/arXiv.2401.07348. 10.
[362] NOVELLI, CASOLARI, HACKER, SPEDICATO, FLORIDI op. cit. 10–11.
[363] Megjegyzendő, hogy a GDPR (47) preambulum-bekezdésével összhangban azonban nem szükséges hozzájárulás bekérése marketing célú adatkezeléshez az adatkezelő és az érintett közti megfelelő kapcsolat esetén, ha az érintett észszerűen számíthat a marketing célú megkeresésre (például: a közelmúltban az adatkezelő webáruházában vásárolt, és a marketingüzenet ehhez hasonló termékekkel kapcsolatos). Ezen szabály alkalmazhatósága azonban kérdéses lehet MI általi, marketing célú profilalkotás esetén, mivel ilyen esetekben az érintett kérdésesen számíthat az adatkezelésre.
[364] Lásd: IAB Europe, TCF – Transparency & Consent Framework, https://iabeurope.eu/transparency-consent-framework/

jogsértőnek találta, a szervezetet pedig 250.000 euró összegű adatvédelmi bírsággal sújtotta.[365] A döntéssel szemben a szervezet jogorvoslattal élt, amelynek keretében az eljáró bíróság előzetes döntéshozatal iránti kérelemmel fordult az EUB-hez. Az ügyben az EUB azt vizsgálta, hogy az érintettek reklámcélú preferenciáit rögzítő numerikus karakterlánc, az ún. „Transparency and Consent String" (TC-string), személyes adatnak tekinthető-e. E körben az EUB arra a megállapításra jutott, hogy „*amennyiben a TC Stringhez hasonló betűk és karakterek kombinációjából álló lánc kiegészítő adatokkal – többek között a felhasználó készülékének IP-címével vagy más azonosítókkal – való összekapcsolása lehetővé teszi e felhasználó azonosítását, meg kell állapítani, hogy a TC String azonosítható felhasználókra vonatkozó információkat tartalmaz*"[366] – így e körben az EUB a fenti adatot személyes adatnak tekintette, amennyiben az más adattal való összekapcsolása révén az érintett azonosításához vezethet.

Ahogy az a fentiekből is látszik, a hozzájárulásnak a fenti követelményeknek való megfelelésen túl megfelelő tájékoztatáson kell alapulnia, ennek hiányában ugyanis az érintett nem rendelkezhet kellő tudással az adatkezelés körülményeiről. Ennek kapcsán az EDPB hozzájárulásról szóló iránymutatása is meghatározást ad a tájékozott hozzájárulás minimumfeltételeiről, ideértve tájékoztatás nyújtását az adatkezelő kilétéről, az adatkezelés céljáról, a kezelt adatok típusáról, a hozzájárulás visszavonásának lehetőségéről, az automatizált döntéshozatal céljából történő felhasználásról, illetve profilalkotásról, valamint a harmadik országba történő adattovábbításra vonatkozó garanciákról.[367] Ezen információkat tehát az adatkezelőnek át kell adnia, vagy azoknak egyértelműen következniük kell az érintett számára a hozzájárulás megadását megelőzően. A fenti hozzájáruláshoz kapcsolódó, „minimális tájékoztatás" nyújtása azonban nem jelenti azt, hogy az adatkezelő mentesülne a tájékoztatással kapcsolatos egyéb kötelezettségei alól, amelyeknek továbbra is meg kell felelnie, illetve azokat jellemzően az érintettek számára is elérhető, vonatkozó adatvédelmi tájékoztatójában meg kell jelenítenie.[368]

[365] Autorité de protection des données, Décision sur le fond 21/2022 du 2 février 2022, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022.pdf, 569.
[366] C-604/22. sz. ügyben hozott ítélet: IAB Europe és a Gegevensbeschermingsautoriteit között [ECLI:EU:C:2024:214] 45. pont
[367] Az Európai Adatvédelmi Testület 5/2020 Iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 1.1 verzió, elfogadás időpontja: 2020.05.04. („**5/2020 Iránymutatás**"), 17–18.
[368] NECZ (2020a) i. m. 11–12.

Kiemelendő továbbá, hogy személyes adatok különleges kategóriáinak kezelése esetén a hozzájárulásnak kifejezettnek kell lennie.[369] A hozzájárulás kifejezettségének követelménye a hozzájárulás kifejezésének módjára, és az érintett kifejezett hozzájárulásának megadásáról való nyilatkozattételére utal. Ez magában foglalja az írásban tett nyilatkozatot, de adott esetben az egyértelmű, elektronikusan (például: elektronikus űrlap kitöltésével, e-mailben), vagy akár az egyértelműen, szóban tett nyilatkozatot is, ha ez utóbbit az érintett megerősíti (például: gombnyomással vagy megerősítést kifejező nyilatkozattal).[370] Így akár az MI általi adatkezelés kapcsán is tehető kifejezett hozzájárulást tartalmazó nyilatkozat az online térben, ha például egy elektronikus űrlap kerül kitöltésre vagy az érintett egyéb kifejezett nyilatkozatot tesz (például adott esetben elektronikus aláírás megtételével). A hozzájárulás kifejezett jellege, valamint a hozzájáruláshoz kapcsolódó további követelmények teljesülése az MI általi adatkezelés kapcsán is az adott eset függvényében vizsgálandó. Ennek kapcsán jellemzően különös jelentőséggel bír az érintett hozzájárulást megelőző megfelelő tájékoztatás megadása, valamint a tájékoztatással és a hozzájárulás megadásával, kezelésével kapcsolatos digitális környezet kialakítása. Amennyiben pedig az érintett fizikai formában megjelenő MI-vel (például: egy szociális vagy kisegítő robottal) folytat interakciót, úgy akár – az eset egyéb körülményeire is tekintettel – kifejezett hozzájárulásnak minősülhet a robot bizonyos részének megérintése.

Napjainkban a hozzájárulás, mint lehetséges jogalap gyakran merül fel a web scraping kapcsán is, tekintve, hogy jellemzően az interneten nyilvánosan elérhető információk gyűjtéséről van szó, amelyet feltételezhetően az érintett hozzájárulásával vagy egyéb jogalapara támaszkodva hoztak nyilvánosságra. Ennek kapcsán felmerülhet a kérdés, hogy ezen eredeti adatkezeléssel összeegyeztethetőnek minősül-e a web scraping céljából történő adatkezelés, figyelemmel a személyes adatok gyűjtésének céljaira, körülményeire, az adatok jellegére, az érintettekre nézve várható esetleges következményekre, kapcsolódó adatvédelmi garanciákra.[371] Mint ahogy a holland adatvédelmi hatóság web scrapinggel kapcsolatos iránymutatása kiemeli, az eredeti adatkezelési cél (például: az adott közösségi médiaoldalon egyes információk nyilvános megjelenítése) és a web scraping által elérni kívánt cél jellemzően elkülönül, ez utóbbit jellemzően szinten eltérő adatkezelők végzik, az adatkezelés pedig számos esetben az érintett számára átláthatatlan marad, igy a web scraping célú adatkezelés a korábbi adatkezelési céllal

[369] GDPR 9. cikk (2) bek. a) pontja
[370] EDPB 5/2020 Iránymutatás, 23-24.
[371] GDPR 6. cikk (4) bek.

jellemzően nem összeegyeztethető, az érintett hozzájárulása pedig a web scraping kapcsán az adatok eredeti nyilvánosságra hozatala kapcsán sem feltételezhető.[372] Mindez azért is érdekes, mivel a francia adatvédelmi hatóság a vonatkozó iránymutatásában megengedőbbnek bizonyult, az eredeti es a tanítóadatok képzése és az e célból történő adatgyűjtés kapcsán pedig az összeférhetőségi teszt elvégzését kulcskérdésnek tekintette.[373] Ennek tükrében az a veszély is fenyegethet, hogy az adatvédelmi hatóságok a web scraping eseten eltérő adatvédelmi követelményeket támasztanak, igy a kérdéskörrel kapcsolatos bizonytalanságokat a közeljövőben vélhetőleg szükséges lesz az EDPB-nek eloszlatnia az egységes joggyakorlat kialakulása érdekében.

A fentiekre tekintettel a holland hatóság általában az egyetlen reális jogalapnak a web scraping kapcsán az adatkezelő jogos érdekét tekinti. Ennek kapcsán azonban a hatóság álláspontja szerint az adatkezelői jogos gazdasági érdekei a web scraping eseten nem írjak felül az érintetti érdekeket, igy csak valamely jogilag méltányolható, jellemzően jogszabályban nevesített adatkezelői érdek indokolhatja ezen jogalapra való hivatkozást a web scraping esetén (például: csalásmegelőzés vagy informatikai biztonság érdekében való adatkezelés).[374] Ezen célok azonban a gyakorlatban jellemzően kevésbé merülnek fel, a web scraping tevékenység pedig a gyakorlatban általában a nagy nyelvi modellek képzésével vagy más üzletileg indokolható céllal van összefüggésben történik. Az iránymutatás kiemeli továbbá, miszerint minél szenzitívebbnek tekinthető a web scraping során gyűjtött adat, annál kevésbé hivatkozható a jogos érdek mint jogalap.[375] Ez a gyakorlatban különösen az egészségügyi célú MI-rendszerek fejlesztése kapcsán jelenthet akadályt, mivel ezen rendszereket jelentős részben kifejezett jogszabályi felhatalmazás hiányában, jogos gazdasági érdek realizálása céljából fejlesztik.

Az érintett jogosult továbbá arra is, hogy a hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása azonban nem érinti a visszavonás előtti adatkezelés jogszerűségét, így tehát ezen korábbi adatkezelést a hozzájárulás visszavonása önmagában nem teszi érvénytelenné vagy jogsértővé. Amennyiben több adatkezelő jár el, és kezel személyes adatot ugyanazon hozzájárulás alapján, úgy e körben elegendő, ha az érintett bármelyik adatkezelőhöz fordul a

[372] Autoriteit Persoonsgegevens, Richtlijnen scraping door private organisaties en particulieren, https://autoriteitpersoonsgegevens.nl/uploads/2024-05/Handreiking%20scraping%20door%20particulieren%20en%20private%20organisaties.pdf ("**Web scraping iránymutatás**"). 10–11.
[373] CNIL AI how-to sheets
[374] Web scraping iránymutatás, 11–12.
[375] Web scraping iránymutatás, 14.

hozzájárulás visszavonása érdekében.[376] Megemlítendő továbbá, hogy a hozzájárulás visszavonását a hozzájárulás megadásához hasonlóan egyszerű módon kell lehetővé tenni.[377] Így például egy virtuális asszisztens részére szóban adott hozzájárulás esetén a visszavonást is szóban kell lehetővé tenni.

A hozzájárulás mellett szintén relatíve gyakran hivatkozott jogalapnak tekinthető az érintettel kötött szerződés teljesítése.[378] E körbe beleértendők az érintettel már megkötött szerződés teljesítéséhez szükséges (például: webáruházból történő rendelés kapcsán a rendelés, szállítási cím kezelése), valamint azon adatkezelési műveletek is, amelyek a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükségesek (például: álláspályázatra jelentkezők adatainak kezelése az adott pozícióra alkalmas jelölt kiválasztása céljából). Hangsúlyozandó azonban, hogy a szerződéses jogalap nem hivatkozható, ha nem közvetlenül az érintettel történik szerződéskötés (hanem például egy gazdasági társasággal vagy egy civil szervezettel, amelynek a nevében a képviselője jár el), illetve abban az esetben sem, ha a szerződéskötést megelőzően az adatkezelő kérésére történő lépések megtételéhez szükséges az adatkezelés, például, ha az adatkezelő keresi meg ajánlattal az érintettet, és az adatkezelésre ezen megkereséssel összhangban kerül sor. Természetesen azonban e körben is lehetnek vitatható esetek, amikor nehezen ítélhető meg, hogy az adott adatkezelés szükséges-e a szerződés teljesítéséhez vagy a szerződéskötést megelőző lépések megtételéhez. Például, ha az adott álláspályázatra az érintett jelentkezik, azonban a toborzás során a jelentkezők előszűréséhez egy MI-alapú szoftveres megoldást használnak, kérdésesen lehet indokolható, hogy a megoldás ténylegesen szükséges a megfelelő jelentkező kiválasztásához, illetve, hogy az érintett „kérése", illetve várakozásai, számításai kiterjednek-e a fenti szoftver alkalmazására, így a szerződéses jogalap ilyen esetekben nem feltétlenül releváns. Ilyen esetben tehát az adatkezelőnek célszerű lehet egyéb jogalapot megjelölnie a vonatkozó MI-alapú előszűréssel kapcsolatos adatkezeléshez (például: jogos érdek, ha az MI ennek kapcsán csak a munkáltatói döntést támogató szerepet tölt be, és önálló döntést nem hoz). Vélhetően a legtöbb szerződéskötést vagy teljesítést támogató megoldás kapcsán napjainkban még hasonló logika érvényesülhet, tekintettel arra, hogy a szerződések többségének létrejöttéhez vagy teljesítéséhez MI-alapú megoldás alkalmazása nem szükséges, az inkább csak támogató jelleggel bírhat. E körben azonban a technológiai fejlődéssel, valamint az egyes MI-alapú megoldások

[376] C-129/21. sz. ügy Proximus NV kontra Gegevensbeschermingsautoriteit [ECLI:EU:C:2022:833] 84. pont
[377] GDPR 7. cikk (3) bek.
[378] GDPR 6. cikk (1) b) pontja

elterjedésével a vonatkozó adatkezelések társadalmi és egyben adatvédelmi megítélése is változhat, így elképzelhető, hogy a közeljövőben bizonyos szerződések létrejöttét vagy teljesítését támogató vagy lehetővé tevő MI-alapú megoldások alkalmazása már a szerződés teljesítéséhez, vagy akár megkötéséhez is szükségesnek, illetve azokkal összefüggő adatkezelésnek lesz tekinthető, és így az adatkezelés jogalapját is ehhez kell majd igazítani. Mindez azonban csak akkor foghat helyt, ha az adott MI-alapú megoldások alkalmazásához megfelelő transzparencia társul, és az adatkezelő ennek tükrében igazolni tudja, hogy a megoldás alkalmazása és a kapcsolódó adatkezelés ténylegesen szükséges a vonatkozó szerződés teljesítéséhez.[379] Megjegyzendő továbbá, hogy nem elégséges jellemzően ezen jogalap hivatkozásához, ha az MI pusztán említésre kerül az adott szerződésben vagy kiegészítő funkcióként segíti a szerződés teljesítését[380] (például: egy ügyintézést megkönnyítő chatbot alkalmazás, amelyet a bank biztosít az ügyfeleinek).

Természetesen a fentebb írtak szerint a szerződéses viszonyokhoz kapcsolódó egyes adatkezelések kapcsán egyéb jogalapok megválasztása adott esetben helyesebbnek tűnhet, mint az adatkezelés szerződés teljesítésére való alapozása. Ilyennek minősülnek például a szerződéses vitákkal, szerződéses követelések érvényesítésével kapcsolatos adatkezelési műveletek, hiszen ezek jellemzően a szerződés nem, vagy nem megfelelő teljesítéséből adódnak,[381] vagy erre vonatkozó állításokkal, igényekkel szembeni védekezéshez szükségesek. Emellett a szerződéses viszonyok teljesítése kapcsán is szükséges lehet bizonyos ehhez tapadó jogszabályi kötelezettségeknek történő megfelelésre (ideértve például: adózási, számviteli kötelezettségeknek, illetve fogyasztókkal kötött szerződések esetén fogyasztóvédelmi jogszabályi követelményeknek való megfelelés), így az erre vonatkozó adatkezelési műveletek is az adatkezelőre vonatkozó jogi kötelezettség, nem pedig magának az alapul fekvő szerződésnek a teljesítéséhez szükségesek.

A fentebb említettek szerint az MI alapú megoldások esetén is indokolt lehet az adatkezelőre vonatkozó jogi kötelezettségeknek történő megfeleléshez szükség adatkezelés,[382] azonban e

[379] Hangsúlyozandó, hogy a munkahelyi adatkezeléssel kapcsolatos egyéb szempontok a tanulmány 4. pont j) ii) pontjában kerülnek ismertetésre.
[380] Pók LÁSZLÓ: Mesterséges intelligencia, személyes adatok és az adatkezelés jogalapjai. *GDPR Blog*, 2023.11.30, https://gdpr.blog.hu/2023/11/30/mesterseges_intelligencia_szemelyes_adatok_es_az_adatkezeles_jogalapjai. [a továbbiakban: PÓK (2023)]
[381] NAIH-3975-1/2021. 9.
[382] GDPR 6. cikk (1) c) pontja

tekintetben értelemszerűen még mind az európai uniós, mind jellemzően a tagállami szabályozás kialakulóban van, így napjainkban kifejezetten MI alapú adatkezelést megkövetelő jogszabályi követelményekről még kevésbé beszélhetünk, és inkább azon esetek tekinthetők relevánsnak, ahol az adott MI-rendszer jogi kötelezettség teljesítését támogatja (például: információk összegyűjtése és továbbítása hatóság részére), vagy ahol azt jogszabályi tilalom hiányában végzik. Adott esetben jogi kötelezettség teljesítésének tekinthető azonban az adatbázis végrehajtási értékesítése során a személyes adatok védelmével kapcsolatos azon előírásnak való megfelelés, amelyet a végrehajtó foglal bele az árverési záradékba, a vásárlóra kötelező módon.[383]

Kérdéses lehet ugyanakkor, hogy egy-egy általánosnak tekinthető jogszabályi felhatalmazás egyben az MI alapú megoldás alkalmazására, és az ehhez kapcsolódó adatkezelésre való felhatalmazásnak is tekinthető-e. Ennek kapcsán maga a GDPR is kiemeli, miszerint a jogi kötelezettség teljesítése érdekében végzett adatkezelések kapcsán nem szükséges, hogy minden egyes adatkezelési műveletre külön jogszabályi rendelkezés vonatkozzon, és több hasonló adatkezelési művelet végzéséhez is alapul szolgálhat akár egyetlen jogszabály, illetve vonatkozó jogszabályi rendelkezés is.[384] Olyan esetekben azonban, ahol valamilyen komplex, az adatkezelés kockázatait felerősítő technológiai megoldás kerül alkalmazásra (ideértve különösen egyes MI alapú megoldásokat), különösen vizsgálandó, hogy szükséges-e specifikus jogszabályi felhatalmazás. Például, egy járvány elleni védekezésre felhatalmazó törvényi rendelkezés kapcsán kérdésként merülhet fel, hogy általános jogszabályi felhatalmazás alapján egy MI alapú megoldással is vizsgálhatók-e kontakt adatok, vagy ebben az esetben az adatkezelés már túlmutat a demokratikusan megengedhető kereteken, esetleg eltérő jogalapra támaszkodás szükség az adatkezeléshez? Elegendő érvként szolgál-e a járvány gyorsabb megfékezésének nagyobb esélye, vagy az érintettek kapcsolatainak, esetleges viselkedésének széleskörű megismerése, és azokba való túlzott állami behatás okán a lehetséges körben adatvédelmi szempontból kevésbé aggályos, és az érintettek jogait és szabadságait kevésbé érintő megoldás alkalmazására van szükség? A fenti kérdések megválaszolásához mindenképp vizsgálandó a jogi kötelezettség pontos meghatározása és természete, valamint az, hogy ennek teljesítéséhez az MI alkalmazása, hogyan viszonyul.[385] Ha az MI alkalmazása adott esetben

[383] C-693/22. sz. ügy Pikamäe főtanácsnok indítványa: I. sp. z o. o. kontra M. W. [ECLI:EU:C:2024:162] 94. pont
[384] GDPR (45) preambulum-bekezdés
[385] PÓK (2023) i. m.

csak járulékosan kapcsolódik a jogi kötelezettség teljesítéséhez, úgy annak alkalmazásával kapcsolatos adatkezeléshez jellemzően egyéb jogalap igazolása szükséges.

Ugyancsak kérdéskénként merülhet fel, hogy egy adott ügyben eljáró bíróság vagy hatóság mennyire intézkedhet MI alapú megoldás alkalmazásáról, illetve mennyire írhatja azt elő. A helyzet megítélése itt is valószínűleg hasonló, mint az MI jogszabályi felhatalmazás alapján történő alkalmazása vonatkozásában. Az olyan kiegészítő, a bíróság vagy a hatóság munkáját támogató megoldásoknál, mint például egy-egy adminisztratív folyamat támogatása vagy bizonyos technikai jellegű szakértői értékelések, az MI vélhetőleg a vonatkozó eljárási rendelkezések keretein belül is alkalmazható, hiszen itt nem veszi át a bíróság vagy a hatóság döntési kompetenciáját, és – feltételezvén, hogy az MI által létrehozott eredmények érdemi, emberi áttekintésére sor kerül –, a bírósági vagy hatósági döntést jellemzően nem befolyásolja jelentős mértékben az MI. Erre példaként szolgálhatnak az egyes adatgyűjtéssel, elemzéssel, szakértői feladatok támogatásával kapcsolatos rendszerek.[386] Kiemelendő azonban, hogy az MI eltérően értelmezhet bizonyos korábbi döntéseket vagy eseteket, így a kutató jellegű vagy döntést támogató MI-rendszereknél fontos lehet nagyobb hangsúlyt helyezni a hivatkozások kontextusának feltérképezésére, valamint az MI által javasolt döntések megmagyarázhatóságára.[387] Emellett a mechanikusnak és statikusnak tekinthető elemzési, mérlegelési folyamatok, valamint az ezekre történő támaszkodás az emberi döntési folyamatban megjelenő empátia szerepének csökkenéséhez is vezethetnek, így az emberi szakértők és az ezen döntéseket felülvizsgálók számára kiemelten fontos a jog és a technológia együttes értelmezése és megfelelő mértékű ismerete.[388]

Olyan esetekben továbbá, ahol a jogalkotó egy-egy állami döntés meghozatalát az MI-re bízza, elengedhetetlen a megfelelő jogszabályi keretrendszer kidolgozása, amely jellemzően magában kell, hogy foglalja az emberi felülvizsgálat lehetőségét is. E körben vélhetőleg először az egyszerűbb adminisztratív, nemperes eljárások kerülnek majd tömegesen automatizálásra (például: egyes adatok bejegyzéssel, hivatalos dokumentumok másolatának lekérésével kapcsolatos ügyek, egyes egyszerűbb eljárások), ezek esetén ugyanis az MI általi tévedés, és az

[386] MISKOLCZI Barna, SZATHMÁRY Zoltán: *Büntetőjogi kérdések az információk korában – mesterséges intelligencia, big data, profilozás*. Budapest, HVG-Orac Lap- és Könyvkiadó Kft., 2018. 190–191.
[387] Jacob Livingston SLOSSER: Artificial Intelligence and Public Law. In: Mariana VALVERDE, Kamari M. CLARKE, Eve Darian SMITH, Prabha KOTISWARAN (eds.): *The Routledge Handbook of Law and Society*. London, Routledge, 2021. 79.
[388] Ron DOLIN: Technology Issues in Legal Philosophy. In: Daniel Martin KATZ, Ron DOLIN, Michael J. BOMMARITO (eds.): *Legal Informatics*. Cambridge, New York, Cambridge University Press, 2021. 23.

abból származó káros hatások kockázata is jellemzően alacsonynak tekinthető. Az érintettek jogaira és szabadságaira kiemelt hatással bíró állami döntések meghozatala és eljárások érdemi lefolytatása a demokratikus társadalmakban azonban a technológia fejlődésével is az emberi döntéshozatal terrénuma kell, hogy maradjon, az MI-nek ilyen esetekben pedig legfeljebb döntést támogató szerepre kell szorítkoznia, abban az esetben is, ha az MI már elég fejlett lesz ahhoz, hogy egy emberi döntéshozó szakértelmével döntsön. Nehezen lenne elfogadható ugyanis, hogy például egy büntetőügyben vagy egy gyermekelhelyezéssel kapcsolatos jogvitában emberi döntéshozók helyett az MI hozzon döntést, hiszen ez az igazságszolgáltatás emberarcúságát kérdőjelezné meg.

Szintén kevésbé tekinthető napjainkban gyakorinak az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükségessé váló adatkezelés MI-rendszer alkalmazása esetén,[389] azonban a technológiai fejlődéssel, és az MI alapú megoldások elterjedésével vélhetően ezen jogalapra való hivatkozás is egyre gyakoribbá válik majd. Például korábban a skót rendőrség vezetett be egy olyan drónrendszert, amely MI-vel támogatva segít azonosítani és megtalálni eltűnt személyeket.[390] Az arcfelismerő és különböző MI-alapú azonosító rendszerek ezen alkalmazása adatvédelmi szempontból is kevésbé tűnik kockázatosnak mint a bűnüldözési célú alkalmazás, tekintettel arra, hogy itt a téves azonosítással járó, érintettet érő negatív hatások enyhébbek, jellemzően pedig az alkalmazás területén (például: erdők vagy egyéb kies, emberi szemszögből nehezen belátható területek) is kevesen tartózkodnak. Így a fentiek tükrében a hasonló, azonosításra és személykeresésre használt alkalmazások kiváló segítséget nyújthatnak például eltűnt vagy bajba jutott kirándulók vagy katasztrófa sújtotta területen tartózkodók azonosításában, illetve megtalálásában (például: árvíz sújtotta területen). Megemlítendő ugyanakkor, hogy az érintett vagy másik természetes személy létfontosságú érdekei MI-rendszer alkalmazása esetén is jellemzően csak eseti jelleggel szolgálhatnak alapul az adatkezeléshez, amíg az érintett az adott helyzetben nem képes jogait gyakorolni, érdekeit képviselni, illetve megvédeni. Így az érintett létfontosságú érdekeinek védelme okán a személyes adatok MI-rendszer fejlesztésé érdekében végzett kezelése jellemzően nem foghat helyt.[391]

[389] GDPR 6. cikk (1) d) pontja
[390] Ken MACDONALD: Police to use AI recognition drones to help find the missing. *BBC News*, Scotland, 2019.11.04. https://www.bbc.com/news/uk-scotland-50262650
[391] AI Discussion paper, Baden-Württemberg V. 4.

A fentieken mellett külön kihívást jelenthet az MI közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása kapcsán végzett adatkezelés körében történő alkalmazása.[392] Mindenekelőtt leszögezendő, hogy ezen jogalap csak bizonyos szervek és személyek számára tekinthető hivatkozási alapnak, amelyek működése közérdekűnek tekinthető, illetve amelyek közhatalom gyakorlására jogosultak. E körbe tartoznak az állami és önkormányzati szervek és hatóságok, valamint a jogszabály által közhatalom gyakorlására felhatalmazott egyéb szervezetek és személyek is. Ezen felhatalmazás a jogi kötelezettségen alapuló adatkezelés kapcsán írtak szerint lehet egy általános törvényi felhatalmazás vagy keretrendszer is,[393] azonban a felhatalmazásnak mindenképpen konkrétnak kell lennie, valamint konkrét címzetthez kell szólnia. Így nem tekinthető például általánosságban a sajtó tevékenységére hivatkozó adatkezelés minden esetben közérdekűnek, azt az adott tevékenységre, kapcsolódó adatkezelésre tekintettel szükséges vizsgálni.[394] Megemlítendő, hogy e körben általában az érintett tájékozott hozzájárulása sem lehet jellemzően megfelelő jogalap,[395] így a médiatartalom-szolgáltatónak és a személyes adatok kezelését végző újságíróknak a jogalap megválasztása, illetve az alapelvek ütközésének feloldása során megfelelő körültekintéssel szükséges eljárniuk.

A közérdekű adatkezelés kapcsán továbbá különös hangsúlyt élvez a tagállami alkotmányjogi követelményeknek és hagyományoknak történő megfelelés fontossága is, hiszen a közérdek, valamint a közhatalom gyakorlása is csak ennek tükrében, ezzel összhangban értelmezhető. Magyarországon például az Alkotmánybíróság 28/2014. (IX. 29.) AB határozatában kiemelte, miszerint „*... képfelvétel hozzájárulás nélkül is nyilvánosságra hozható, ha a nyilvánosságra hozatal nem öncélú, vagyis az eset körülményei alapján a jelenkor eseményeiről szóló vagy a közhatalom gyakorlása szempontjából közérdeklődésre számot tartó tájékoztatásnak, közügyet érintő képi tudósításnak minősül*”.[396] Érdekes belegondolni, hogy mindezen logika vonatkoztatható-e a fentiek szerint készült felvételek további MI általi felhasználására, és arra sor kerülhet-e az eredeti közérdekű adatkezeléssel kapcsolatos jogalap alapján, vagy annak kapcsán külön jogalap hivatkozása szükséges. Ezen kérdés álláspontunk szerint az MI általi

[392] GDPR 6. cikk (1) bek. e) pontja
[393] GDPR (45) preambulum-bekezdés
[394] BH 2022.7.189. [144] bek.
[395] PÉTERFALVI Attila, OSZTOPÁNI Krisztián: A személyes adatok magánjogi védelme a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatában. In: GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András: *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017. 392–393.
[396] 28/2014. (IX. 29.) AB határozat [43]

adatkezeléssel kapcsolatos esetleges további adatkezelési cél függvényében dönthető el. Ha azonban a további adatkezelés az eredetitől elkülönül, úgy adott esetben további jogalap (például adott esetben az adatkezelő jogos érdeke) hivatkozása lehet szükséges.

Az MI alapú adatkezelések esetén különös jelentősége van továbbá az adatkezelő vagy valamely harmadik fél jogos érdekére történő hivatkozásnak. A jogos érdek akkor állhat meg, „*ha az adatkezelő 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*”.[397] Ennek kapcsán az adatkezelővel szemben alapvető elvárás valamennyi jogos érdeken alapuló adatkezelése esetén a jogos érdek dokumentált érdekmérlegelési tesztben történő alátámasztása, valamint annak az adatvédelmi tájékoztatóban való összefoglalása is.[398]

Az érdekmérlegelési tesztben az adatkezelőnek egyértelműen meg kell határoznia az adatkezelői érdeket, az azzal szemben álló érintetti érdeket, valamint ezeket össze kell mérnie, megadva az érdekmérlegelési teszt eredményét, és ezzel megválaszolva azt a kérdést is, hogy az adatkezelői érdek az adott esetben felülírja-e az érintetti érdekeket.[399] Ehhez azonban az érdekmérlegelési tesztnek meg kell jelenítenie az adatkezelés érintett jogaira és szabadságaira jelentett veszélyeit és kockázatait, valamint az azok kiküszöbölésére, csökkentésére szolgáló intézkedéseket.[400] Jelentős szempontnak tekintendő továbbá az MI alkalmazásával kapcsolatos érdekmérlegelési tesztben az MI általi adatkezelés szükségességének (például: szintetikus vagy anonimizált adatok felhasználása az adott esetben elégtelen), valamint arányosságának igazolása, ideértve annak figyelembevételét is, hogy az érintett mennyire számíthat az MI alkalmazására az adott körülmények között, illetve az adatkezelővel való kapcsolatára tekintettel.[401]

Kiemelendő azonban, hogy az MI alapú adatkezelések esetén az adatkezelői jogos érdek, valamint annak érintetti érdekekkel való összevetése különös gonddal vizsgálandó, tekintettel az MI alapú adatkezelések sajátosságaira (különösen azok sokszor nehézkes áttekinthetőségére, az MI adatéhségére, alkalmazásának átfogó hatásaira és eredményeire, a technológia

[397] GDPR 21. cikk (1) bek.
[398] GDPR 13. cikk (1) d), valamint (2) b) pontjai
[399] Lásd: NAIH/2020/1154/9. 39.
[400] Lásd: NAIH/2019/55/5. 17.
[401] PÓK (2023). i. m.

fejlődésével kapcsolatos bizonytalanságokra). Ennek kapcsán figyelembe veendő továbbá, hogy a legtöbb adatkezelési cél jellemzően MI-rendszerek alkalmazása nélkül is elérhető, az adatkezelő gazdasági érdekei és üzleti elvárásai pedig általában ritkábban írják felül az érintetti érdekeket, különösen az új technológiák alkalmazása esetén, amelyek az érintettek magánéletére sokszor nagyobb behatással bírnak, vagy számukra jelentős döntések meghozatalához vezetnek. Az MI-rendszerek alkalmazása ezen esetben az érintettek személyes adatok védelméhez fűződő joga melletti további személyiségi jogai tekintetében is jelentős korlátozáshoz vezethet, amely az érdekmérlegeléskor szintén figyelembe veendő.[402] Mindemellett bizonyos területeken az MI alkalmazása különös garanciákat kíván az alkalmazási terület sajátosságaira, valamint egyéb társadalmi, etikai szempontokra tekintettel, ideértve például az MI egészségügyi kutatások területén való alkalmazását. Kevésbé merülnek fel azonban a fenti aggályok, ha az MI inkább adminisztratív, kisegítő szerepben kerül alkalmazásra, ahol az adatkezelés alapvetően MI megoldás alkalmazása nélkül is megvalósulhatna, az MI alkalmazása azonban csak megkönnyíti vagy hatékonyabbá teszi azt. Erre jó példának tekinthetők a jogi piacon elterjedt különböző dokumentumok elemzésére szolgáló megoldások, amelyek segítségével például egy-egy ügyvédi iroda hatékonyabban képes egy peres eljárás nagyszámú dokumentációját áttekinteni.

Kiemelendő, hogy amennyiben marketing célból kerül sor a jogos érdeken alapuló adatkezelésre, úgy az érintett tiltakozása esetén az adatkezelést haladéktalanul meg kell szüntetni, az érintett ezirányú döntési joga ugyanis az adatkezelő marketing érdekei felett áll.[403] Marketing célú adatkezelésnél továbbá az MI alkalmazása vélhetőleg kevésbé, illetve inkább csak az érintett előzetes hozzájárulása alapján foghat helyt, tekintettel arra, hogy az érintettek kevésbé számíthatnak arra, hogy a részükre marketing célú megkeresést, illetve ajánlatokat MI alkalmazása – különösen profilalkotás – révén, illetve alapján intéznek. A technológia, valamint a kapcsolódó társadalmi elvárások változásával azonban e tekintetben is változások képzelhetők el.

e. A mesterséges intelligencia és a különleges adatok kezelése

Az MI alkalmazása esetén különös kihívást jelent a szenzitív információk védelme, ideértve például az érintettek egészségügyi adatait, politikai véleményére vagy vallási meggyőződésére

[402] PÉTERFALVI, OSZTOPÁNI i.m. 393.
[403] GDPR 21. cikk (1)-(2) bekezdései

vonatkozó adatokat, tekintettel arra, hogy a nagy mennyiségű szenzitív információ MI általi kezelése jelentős kockázattal bírhat az érintett számára,[404] így például az érintettre vonatkozó profilalkotáshoz is alapul szolgálhat, adott esetben az érintett sebezhetőségének kihasználásához, valamint diszkriminatív döntések meghozatalához vezethet. Emellett akár az érintett egyes szokásai, vagy önmagukban szenzitívnek nem tekinthető jellemzői alapján is adott esetben könnyen vonhat le az MI az érintett szenzitív tulajdonságaira vonatkozó következtetéseket (ideértve például az érintettek vásárlási, illetve felhasználói szokásait). E körben egyes kiskereskedelmi szolgáltatók algoritmusai például a vásárlók terhességét is képesek lehet nagy valószínűséggel felismerni, akár korábban is, mint maguk az érintettek vagy családtagjaik.[405]

Figyelemmel az érintettek nagyobb fokú kiszolgáltatottságára szenzitívnek tekinthető információik kezelése esetén, a GDPR az érintettek szenzitív, ún. különleges adatainak kezelését csak meghatározott feltételek teljesülése esetén teszi lehetővé. Ezen feltételek egyben „többletfeltételnek" is tekinthetők, hiszen a személyes adatok kezelésére irányadó egyéb feltételek (például: adatkezelési cél meghatározása, megfelelő jogalap megléte, stb.) mellett kell fennállniuk ahhoz, hogy az adott különleges adat kezelhető legyen. Emellett kivételnek is tekinthetők a különleges adatok kezelésének általános tilalma alól, tekintettel arra, hogy ilyen releváns „kivétel" igazolása nélkül különleges adatok nem kezelhetők. Ilyen kivételes adatkezelésnek tekinthető különösen az érintett kifejezett hozzájárulása alapján végzett,[406] az érintett foglalkoztatásával kapcsolatos,[407] jogi igények érvényesítésével, védelmével kapcsolatos,[408] közérdekből végzett,[409] adott esetben egészségügyi célú,[410] valamint a közérdekű archiválási, kutatási, statisztikai célból végzett adatkezelés,[411] továbbá néhány egyéb specifikus helyzetben végzett adatkezelés is (ideértve például az érintett vagy más személy létfontosságú érdekében végzett adatkezelést[412]).

[404] PÓK (2023). i. m.
[405] Kashmir HILL: How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. *Forbes*, 2012.02.16, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
[406] GDPR 9. cikk (2) a) pontja
[407] GDPR 9. cikk (2) b), h) pontjai
[408] GDPR 9. cikk (2) f) pontja
[409] GDPR 9. cikk (2) g) pontja
[410] GDPR 9. cikk (2) h), i) pontjai
[411] GDPR 9. cikk (2) j) pontja
[412] GDPR 9. cikk (2) c) pontja

Hangsúlyozandó, hogy a fenti kivételek nem feleltethetők meg minden esetben a GDPR-ban meghatározott jogalapoknak, azoktól adott esetben eltérő vagy azokhoz képest többlet-követelményeket határozhatnak meg. Így például a jogalapok körében a GDPR a „hozzájárulást", míg a különleges adatok kezelésének általános tilalma alóli kivételként már a „kifejezett hozzájárulást" említi. A kivételek közül hiányzik továbbá a szerződéskötéshez szükséges adatkezelés, valamint – a jogi igények előterjesztésével, érvényesítésével, védelmével kapcsolatos adatkezelésen túlmenően – a jogos érdek alapján történő adatkezelés. Nem találunk továbbá az MI-vel kapcsolatos kivételeket sem, holott az MI fejlesztésével kapcsolatos, valamint egyes MI alkalmazásával járó adatkezelések ezt adott esetben megkövetelhetnék. Így a GDPR jelenlegi szabályai alapján az esetek jelentős részében, illetve különösen a gazdasági érdekből, üzleti célból történő felhasználás esetén jellemzően csak az érintett kifejezett hozzájárulására támaszkodhat reálisan az adatkezelő a különleges adatok MI általi kezelése kapcsán, ugyanis az érintetti és adatkezelői érdek összemérésére és az adatkezelő jogos érdeke alapján történő adatkezelésre ilyen esetekben nincs lehetőség, a kutatási célú adatkezelések kapcsán pedig a GDPR a kutatási célú (GDPR 9. cikk (2)(j) pontja), és nem az üzleti felhasználást preferálja.[413] Hangsúlyozandó továbbá, hogy a szerzői jog által védett tartalmakat érintő szöveg- és adatbányászat kapcsán az európai uniós jogban rendelkezésre álló felhasználási kivételek[414] nem állnak rendelkezésre az adatvédelem területén, erre tekintettel tanácsosnak tűnne a GDPR 9. cikke alóli további kivételek bevezetése, például az egészségügy, az oktatás vagy a foglalkoztatás területén.[415]

Hangsúlyozandó továbbá, hogy az olyan esetekben, ahol ez a nagy kockázatú MI-rendszerekkel kapcsolatosan a torzítás észlelésének és korrekciójának biztosításához feltétlenül szükséges, az ilyen rendszerek szolgáltatói kivételesen kezelhetik többek között az érintettek különleges adatait is, amennyiben – az MI Rendeletben ennek kapcsán meghatározott – vonatkozó feltételek teljesülnek (így például: a torzítás észlelése és korrekciója más típusú, például szintetikus vagy anonimizált adatok felhasználásával nem lehetséges, az adatok újbóli felhasználása korlátozott, megfelelő adatbiztonsági intézkedések kerültek alkalmazásra, az adatok nem kerülnek továbbításra más személyeknek).[416] Így tehát az MI Rendelet külön

[413] NOVELLI, CASOLARI, HACKER, SPEDICATO, FLORIDI op. cit. 10.
[414] Lásd: Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, PE/51/2019/REV/1, HL L 130., 17/05/2019, p. 92–125 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV), 3. és 4. cikkei
[415] NOVELLI, CASOLARI, HACKER, SPEDICATO, FLORIDI op. cit. 10.
[416] MI Rendelet 10. cikk (5) bek.

felhatalmazást ad e körben a különleges adatok kezelésére. Mindezen rendelkezések azonban már kérdésesen alkalmazhatók a különleges adatok hirdetési célú összesítése, elemzése kapcsán. A Maximilian Schrems kontra Meta Platforms Ireland Limited ügyben az EUB – többek között – azt vizsgálta, hogy egy nyilvános közvetített pódiumbeszélgetés során tett, a szexuális irányultságra vonatkozó nyilatkozatot lehet-e akként értelmezni, amely a Facebook vagy hasonló platform számára a szexuális irányultság célzott (például: hirdetési célú) szűrésére, illetve célzott hirdetés céljából való összesítésére és elemzésére is hozzájárulást ad. E körben Ranthos főtanácsnoki indítványában akként foglalt állást, miszerint a nyilvánosan közvetített pódiumbeszélgetés során tett nyilatkozat révén a nyilatkozó kifejezetten nyilvánosságra hozta, és e körben lehetővé tette a szexuális irányultságára vonatkozó különleges adat kezelését.[417] Megjegyzendő azonban, hogy az érintett ezen nyilatkozatával ugyan lehetővé tette a különleges adatok kezelését, azonban a vonatkozó adataira attól függetlenül alkalmazandók a személyes adatok védelmére vonatkozó rendelkezések, hogy azt nem esik a különleges adatok kezelésének tilalma alá,[418] ezen adatok tekintetében pedig nem vezethető le a fentiek szerinti összesítés és elemzés céljából történő hozzájárulás önmagában a fenti, platformon kívül tett nyilatkozat megtételével.[419] A fentiek során a főtanácsnok e körben különös jelentőséget tulajdonított annak a ténynek, hogy az adott platformon kívül tett magatartásra vonatkozóan történt az adatkezelés, így az érintettnek a platformon tett magatartásaival, beállításaival nem volt lehetősége kifejezni a döntését, amelyet a platform számára adott hozzájárulásként lehetett volna értelmezni a fenti adatok összesítésével és elemzésével kapcsolatos kezeléséhez;[420] e körben ugyanis a platform használata során (például: regisztrációkor) megadott különleges adatok a platform szolgáltatója által kerülnek kezelésre, illetve közvetlenül a részére kerülnek megadásra, különbözően a fenti, platformon kívülről származó adatoktól.[421]

f. Az érintetti jogok gyakorlása

Az érintetti jogok jelentős szerepet játszanak a személyes adatok védelme területén, segítségükkel ugyanis az érintettek alapvető információkat szerezhetnek személyes adataik

[417] C-446/21. sz. ügy Ranthos főtanácsnok indítványa: Maximilian Schrems kontra Meta Platforms Ireland Limited, korábban Facebook Ireland Limited [ECLI:EU:C:2024:366] 41–43. pontok, 46. pont
[418] Uo. 46. pont
[419] Uo. 38, 48. pontok
[420] Uo. 36 – 37. pontok
[421] C-252/21. sz. ügy Meta Platforms Inc. és társai kontra Bundeskartellamt [ECLI:EU:C:2023:537] 73. pont

kezeléséről, valamint döntéseket hozhatnak személyes adataik kezelésével kapcsolatban. Ezen jogok gyakorlása technológiai környezetben különösen jelentős szerepet tölt be, tekintettel arra, hogy az érintettek jellemzően kiszolgáltatottabbak az ezen területen aktív adatkezelők számára, illetve adatkezelői közreműködés nélkül kevésbé képesek hatékonyan áttekinteni személyes adataik kezelését, illetve jogaikat és érdekeiket megfelelően érvényesíteni az adatkezelőkkel szemben.

Hangsúlyozandó, hogy az angolszász szabályozás elsődlegesen a magánéletet védő, állami behatást korlátozó *privacy* megközelítésével szemben az európai szabályozás az érintettre vonatkozó személyes adatok védelmét célozza,[422] amelyhez jellemzően – például a magyar alkotmánybírósági gyakorlat tükrében – információs önrendelkezési jogot rendel az érintett számára. Ezen jog nem csak tisztán védelmi jogként érvényesül, hanem egyúttal megteremti annak a lehetőségét is, hogy az érintett maga rendelkezhessen személyes adatai kezeléséről.[423] Ennek tükrében az információs önrendelkezés joga jellemzően kapcsolódik ugyan a magánszférához való joghoz, a társadalmi folyamatokra tekintettel bizonyos esetekben azonban korlátozható.[424]

A GDPR – korábbi nemzetközi és jogtörténeti előzményekre támaszkodva, valamint a személyes adatok fentiek szerinti védelmét célul tűzve – széleskörben biztosítja az adatvédelmi jogok gyakorlását az adatkezelés által érintett személyek számára, és az alábbi érintetti (adatvédelmi) jogokat ismeri el:

- tájékoztatáshoz való jog
- hozzáférési jog
- helyesbítéshez való jog
- törléshez való jog
- az adatkezelés korlátozásához való jog
- adathordozhatósághoz való jog
- tiltakozáshoz való jog

[422] A *privacy* és annak adatvédelemhez való viszonya kapcsán lásd: FREIDLER Gábor: A személyes adatok védelméhez való jog jelentése. In: DÓSA Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., 2008. 20.
[423] 3110/2013. (VI. 4.) AB határozat [50] bek.
[424] 32/2013. (XI. 22.) AB határozat [88] bek.

- automatizált döntéshozatallal, valamint profilalkotással kapcsolatos egyes speciális jogok.[425]

A fenti jogok széleskörben biztosítják az érintettek számára egyrészt, hogy átláthassák személyes adataik kezelését, másrészt, hogy személyes adataik kezelésével kapcsolatosan kinyilváníthassák akaratukat, és adott esetben kifejthessék véleményüket, vagy akár az adatkezelés korlátozásáról, illetve megszüntetéséről is dönthessenek. Mindezen jogok az MI általi adatkezelések esetén is kiemelt jelentőséggel bírnak, különös tekintettel az adatok könnyebb és nagyobb mértékű felhasználására, valamint az adatkezelési műveletek nehezebb átláthatóságára. A technológia sajátosságaira, valamint az annak alkalmazásával kapcsolatos egyes kockázatokra tekintettel azonban az MI általi adatkezelést folytatóknak kiemelt figyelmet kell fordítaniuk az érintettek tájékoztatására, valamint az érintetti jogok gyakorlásának támogatására.

i. A tájékoztatáshoz és a hozzáféréshez való jog

Az érintettek adatvédelmi jogai kapcsán a tájékoztatáshoz való jog kiemelt szerepet játszik, ugyanis lehetővé teszi az érintettek számára, hogy a személyes adataik kezelését áttekinthessék, és ezt követően megfelelően gyakorolhassák további adatvédelmi jogaikat. A tájékoztatáshoz való jog emellett szoros összefüggést mutat az átláthatóság alapelvével, ugyanis az adatkezelőktől alapelvi szinten elvárható, hogy a személyes adatok kezelése során transzparens módon járjanak el. Tekintettel arra, hogy az érintettek tájékoztatásával kapcsolatos követelményekről és szempontokról már fentebb az MI-vel folytatott adatkezelések áttekinthetősége kapcsán írtunk, így ennek megismétlésétől eltekintünk.

A technológiai környezetben végzett adatkezelések esetén szintén kiemelt jelentőséggel bír a hozzáféréshez való jog gyakorlása. A hozzáféréshez való jog keretében az érintett jogosult arról tájékoztatást kapni, hogy adatainak kezelése folyamatban van-e, ha pedig igen, úgy joga van adataihoz hozzáférni.[426] Így amennyiben egy érintett személyes adatait egy részvételével zajló MI-vel támogatott kutatás céljára használják, úgy az érintettnek joga van arról tájékoztatást kapni, hogy az adatait felhasználják-e, például a kutatás későbbi fázisában is, illetve egyéb célokból, és a vonatkozó adataihoz is hozzáférhet. Az érintett hozzáférési joga MI általi

[425] GDPR 1-22. cikk
[426] GDPR 15. cikk (1)–(2) bekezdései

adatkezelés esetén továbbá kiterjedhet az adott modell, illetve annak implementálását követően az adott MI-rendszer felhasználásának különböző fázisaira is,[427]

Érdemes megemlíteni továbbá, hogy a svéd adatvédelmi hatóság a Spotify nevű online zenei szolgáltatóval szembeni eljárást lezáró, 2023-as döntésében külön kiemelte, miszerint megfelelő lehet, ha a hozzáférési jogok gyakorlását a szolgáltató online környezetben külön csoportokra bontva teszi lehetővé. A hozzáférési jogok gyakorlásával kapcsolatos gyakorlata során ugyanis a Spotify külön csoportokra bontva tette lehetővé, hogy a felhasználók hozzáférhessenek adataikhoz, ideértve például a Spotify által leglényegesebbnek vélt felhasználói adatokat (elérhetőségi és fizetési adatok, követett előadók, valamint az adott időszakra vonatkozó lejátszási lista), valamint az általában a felhasználók által kevésbé lényegesnek vélt technikai adatokat (ideértve: log fájlok). A hatóság ennek kapcsán külön megjegyezte, hogy ezen megközelítés jellemzően meg is könnyítheti az érintett számára hozzáférési joga gyakorlását, ugyanis átláthatóbbá teszi számára a róla kezelt, adott esetben nagyszámú adatokat,[428] habár ennek teljesíthetősége a gyakorlatban sok esetben kérdéses lehet.

A hozzáféréshez való jog részét képezi a másolatkéréshez való jog is, amely kapcsán az érintett elektronikusan benyújtott kérelme esetén főszabály szerint az érintett információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani. Az EUB legújabb gyakorlata e körben azt is világossá tette, hogy a másolatkéréshez való jog magában foglalja, hogy az érintett „*változatlan és érthető reprodukciót kapjon*" a másolatkérés által érintett adatokról, amely adott esetben magában foglalhatja dokumentum-kivonatokról, sőt akár teljes dokumentumokról vagy adatbázis-kivonatokról történő másolatigénylést is.[429] Mindezen követelmények az MI általi adatkezelést végzőkre is irányadók lehetnek, így az ilyen adatkezelőknek is például másolatot kell az érintett kérelmére rendelkezésre bocsátaniuk az MI-rendszerhez kapcsolódó adatbázisban tárolt adatokról, adott esetben a vonatkozó kivonat szolgáltatásával, ezeket azonban a szolgáltatók nem mindig lehetnek képesek teljesíteni (ideértve, ha például az adott információk egyébként is az érintett rendelkezésére állnak vagy könnyen elérhetők, és csak aránytalan sérelemmel lehetnének az adott modellből kinyerhetők).

[427] AEPD GDPR Compliance Introduction, 24.
[428] Swedish Authority Against Privacy Protection, Administrative fee against Spotify
[429] C-487/21. sz. ügy F. F. kontra Österreichische Datenschutzbehörde, a CRIF GmbH részvételével [ECLI:EU:C:2023:369] 45. pont

Kiemelendő azonban, hogy a másolatkéréshez való jog nem érintheti hátrányosan más személyek jogait és szabadságait.[430] Így tehát az érintettre vonatkozó másolat feleslegesen vagy indokolatlan mértékben, illetve módon nem tartalmazhat más személyekre vonatkozó információt, azonban a másolat kiadásához való jog gyakorlása kamerafelvételek esetén nem korlátozható kizárólag az érintettet ábrázoló felvételekre;[431] az adatkezelőnek így tehát a kérelem elbírálása során fel kell mérnie a másolat kiadása kapcsán a kérelmezőre és az egyéb érintettekre járó esetleges negatív hatásokat. Így, ha az érintett például a rá vonatkozó, egy adott napon rögzített kamerafelvétel kiadását kéri, helytelen gyakorlatnak tekinthető, ha az adatkezelő az egész napra vonatkozó felvételeket kiadja az érintett részére, hiszen ez számos más személyre vonatkozó felvételt is tartalmazhat, akik ugyanazon a napon látogatták az adott létesítményt. Ilyenkor helyesebb gyakorlatnak tekinthető, ha – az érintett kérelmében foglaltakat is figyelembe véve – csak az érintett látogatására vonatkozó felvétel kerül kiadásra az érintett részére. Ilyen esetben jellemzően az sem jelent problémát, ha a felvétel olyan személyekre vonatkozóan is tartalmaz információt, akikkel az érintett látogatása alatt találkozott, hiszen ez nem jelent új információt a számára, illetve legfeljebb csak kisebb mértékben korlátozza a további érintettek személyes adatainak védelméhez való jogát.[432] Mindez értelemszerűen arcfelismerő, arcképelemző megoldásokkal támogatott kamerarendszerek esetén is alkalmazandó lehet a felvételekre vonatkozóan, a felvételeken szereplő további érintettekre vonatkozó esetleges egyéb információk (például: más személyek azonosítása bűncselekmények áldozataként) azonban már nem szolgáltathatók az ilyen információkhoz hozzáférésre nem jogosultak részére.

Kiemelendő továbbá, hogy az adatkezelő egyes érdekei is a másolatkéréssel kapcsolatos igény teljesítése ellen hathatnak. Ilyennek lehetnek például az adatkezelő szellemi tulajdon vagy üzleti titok védelmével, információbiztonsággal vagy vagyonvédelemmel kapcsolatos érdekei, amelybe napjainkban beletartozhatnak a különböző szervezeti-szervezési, illetve marketing információk, MI-vel vagy egyéb szoftveres megoldások felhasználásával, védelmével, adatkezelési stratégiákkal kapcsolatos információk is.[433] Ezek azonban jellemzően nem írják felül az érintett érdekeit és jogszerű elvárásait, illetve nem vezethetnek a másolatkéréshez való jog teljes megtagadásához, kiüresítéséhez. Így például az adatkezelő nem tagadhatja meg az

[430] GDPR 15. cikk (3)-(4) bekezdései
[431] NAIH/2020/2204/8h 11.
[432] NAIH/2019/1859. 11.
[433] DARÁZS Lénárd: Innováció üzleti titok és know-how hasznosítás útján. *Magyar Tudomány*, 2022/9. 1205.

érintett másolat kiadása iránti kérelmének teljesítését általánosságban az adott MI-rendszerhez kapcsolódó szellemi tulajdonának védelmére hivatkozással.[434] Tekintettel azonban arra, hogy az érintett másolatkéréshez való joga korlátlanul, az adatkezelő vagy mások érdekeinek teljes figyelmen kívül hagyásával nem gyakorolható, lehetőség van arra, hogy az érintettől az adatkezelő pontosítást kérjen a kérelme által érintett adatkör kapcsán, vagy a kifejezetten szellemi tulajdonának, üzleti titkának védelmét szükségessé tevő részeket kitakarja. Megemlítendő továbbá, hogy általában nem gyakorolható a másolatkéréshez való jog a biztonsági mentések esetén, ezek ugyanis az „eredeti" adatok helyettesítésére szolgálnak egy adott biztonsági esemény bekövetkezése esetén (például: adatok elvesztése külső támadás esetén),[435] így vélhetően egy MI-rendszerhez kapcsolódó biztonsági mentés esetén sem gyakorolhatná az érintett hozzáférési jogát, hiszen ezen joga elsődlegesen az egyébként „aktív" adatkészlet kapcsán illeti meg. Ez azonban nem jelenti azt, hogy az érintett jogai feltétlenül korlátozottak lennének, ha egy őt azonosító információ több adatkészletben is szerepel, illetve az érintettet a tájékoztatáshoz való jog is megilleti, akár a biztonsági mentések készítése céljából végzett adatkezelés kapcsán is.

Hangsúlyozandó továbbá, hogy az adatkezelő az érintett által kért első másolatért nem számíthat fel díjat, azonban az érintett által kért további másolatokért az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel.[436] Ennek pontos összege kapcsán egységes mértékről, számítási módról nem beszélhetünk, így ezt az adatkezelőnek szükséges megállapítania az észszerűen felmerülő költségek figyelembevételével. Azon költségek tehát, amelyek egyébként is felmerülnének az adatkezelő tevékenységének végzése során, illetve olyan tevékenységek, amelyek nem járnak különösen, önállóan értékelhető költségvonzattal, jellemzően nem tartoznak ebbe a kategóriába, illetve ennek kapcsán nem vehetők figyelembe. Így például, ha az adott platform vagy az ahhoz kapcsolódó MI megoldás képes az érintett részére könnyen szolgáltatni az általa elektronikusan kért adatokat, úgy akár rövid időn belüli többszöri kérelem esetén sem számítható fel általában díj, hiszen a kérelmet az adatkezelő különösebb nehézségek nélkül teljesíteni tudja. Megemlítendő továbbá, hogy a fentiek szerinti

[434] Lásd: NAIH-3151-2/2021. sz. ügyben hozott határozat. 11.
[435] DPC, Should back-up data be considered as part of an access request?, https://www.dataprotection.ie/en/faqs/access-and-rectification/should-back-data-be-considered-part-access-request
[436] GDPR 15. cikk (3) bek.

díj felszámítása kizárólag a további másolatok igénylése kapcsán lehet releváns, pusztán további tájékoztatás nyújtása esetén nem.[437]

ii. A helyesbítéshez és a törléshez való jog

Az érintettet továbbá az MI általi adatkezelés esetén is megilleti a helyesbítéshez való jog a pontatlan személyes adatok kezelése esetén. A helyesbítéshez való jogba beletartozik továbbá a pontatlan személyes adatok mellett a hiányos személyes adatok, például kiegészítő nyilatkozat alapján történő, kiegészítése,[438] így tehát a helyesbítéshez való jog kiterjedhet valamennyi kisebb, például elírásból származó, vagy akár nagyobb hibára, amely hatással lehet az érintett helyzetére,[439] az érintett ezen joga pedig ezen hibák kapcsán szolgálhat orvosolásul. Így például, ha az érintett részt vesz egy nyelvészeti kutatásban, ahol egy adott ország vagy terület különböző régióiból származók által alkalmazott kifejezésmódot és íráskészséget elemzik MI-rendszer segítségével, úgy az érintett jogosult kérni az ennek kapcsán tévesen felvett adatainak helyesbítését (például, hogy egy mások régióból származik, mint amely vele kapcsolatban nyilvántartásra került). Az érintett azonban jellemzően nem jogosult olyan korábbi információk kijavítására, amelyek rögzítésük vagy egyéb kezelésük esetén pontosak voltak, és amelyek megőrzése szükséges (például: a kutatáskori lakóhely vagy származási régió). Megjegyzendő továbbá, hogy az érintettel kapcsolatos elavultnak tekinthető vagy már nem releváns információk eltávolítása kapcsán inkább az érintett elfeledtetéshez fűződő jogának gyakorlása tekinthető alkalmasnak (például: az érintettre vonatkozó elavult információkat tartalmazó cikk eltávolítása a keresőprogram segítségével elérhető találatok közül). Az MI-rendszerek által generált egyes további információk, például a rendszer által feltárt összefüggések, vagy a rendszer előrejelzései esetén az érintett helyesbítéshez való jogának gyakorlása szintén kérdésesen foghat helyt, tekintettel arra, hogy ezen információk jellemzően inkább szubjektívnek tekinthetők, mintsem tényszerűnek (például: hiteligénylés valószínűsége egy adott időszakon belül).[440]

[437] BUZÁS Péter: Az érintett jogai. In: PÉTERFALVI Attila, RÉVÉSZ Balázs, BUZÁS Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary Kft., 2021, második, átdolgozott kiadás. 198.
[438] GDPR 16. cikk
[439] BUZÁS i. m. 213.
[440] Sandra WACHTER, Brent MITTELSTADT: A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review*, 2019(2). 548–549.

Kiemelendő továbbá, hogy adott esetben akár elavultnak vagy tévesnek tekinthető információk megőrzéséhez is fűződhet az érintetti érdekeket felülíró adatkezelői érdek, ez pedig különösen igaz lehet egyes MI alapú kutatásokra, ha az adott kutatási eredmények, kapcsolódó információk megőrzése az érintett számára különösebb kárt, illetve érdeksérelmet nem okoz, azonban az az adatkezelő számára kifejezetten szükséges vagy hasznos lehet a kutatás további folytatásához, az esetleges későbbi hibák elkerüléséhez. Ugyancsak különös jelentőséggel bírhat a korábbi, adott esetben elavult vagy téves információk kezelése az MI további fejlesztése kapcsán. Így például az érinttet tévesen azonosító chatbot alkalmazás fejlesztése kapcsán a téves azonosításra vonatkozó információk megőrzése is szükséges és releváns lehet, hiszen ezek segítségével a téves azonosítással járó esetek könnyebben elkerülhetők, az alkalmazás pedig továbbfejleszthető.[441] Ilyen esetekben azonban javasolt lehet a vonatkozó információkat anonimizálni, vagy ha ez szükséges, bizonyos ideig maszkolás vagy egyéb hasonló eljárás útján álnevesíteni, szintetikus adatokkal helyettesíteni.

A törléshez, vagy elfeledtetéshez való jog is releváns lehet továbbá az MI általi adatkezelések esetén. Ezen jog kapcsán az érintett jogosult arra, hogy személyes adatainak törlését kérje olyan esetekben, amikor

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
- az érintett a hozzájárulását visszavonja,
- az érintett tiltakozik az adatkezelés ellen, amelyre nem áll fenn elsőbbséget élvező, jogszerű ok, amely az adatkezelést alátámasztaná,
- a személyes adatokat jogellenesen kezelték,
- a személyes adatokat az adatkezelőre irányadó jogi kötelezettség teljesítése érdekében törölni kell,
- a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.[442]

Ahogy az a fentebb írtakból is látszik, az elfeledtetéshez való jog gyakorlása szempontjából kiemelt jelentőséggel bír az adatmegőrzési idő meghatározása. Az adatmegőrzési időt számos esetben jogszabály határozza meg, ideértve például az adózási, számviteli, társadalombiztosítási, munkavédelmi, egyéb foglalkoztatással kapcsolatos, illetve

[441] Lásd: NECZ (2022b) i. m. 102–106.
[442] GDPR 17. cikk (1) bek.

fogyasztóvédelmi jogszabályi rendelkezéseket. Természetesen azonban egyéb sajátos területeken, illetve tevékenységek kapcsán is határozhat úgy a jogalkotó, hogy bizonyos adatok, illetve dokumentáció, vagy akár hang- és képfelvételek megőrzését meghatározott időtartamra előírja, jellemzően az adatkezelő ellenőrizhetősége, valamint az esetleges viták megelőzése, bizonyítékok megőrzése érdekében. A fentiekhez hasonlóan bíróságok vagy egyéb hatóságok is előírhatnak adatmegőrzést egyedi esetben, ha az például az adott eljárás kapcsán bizonyítási vagy egyéb célból szükséges (például: kamerafelvétel megőrzésének elrendelése). Hasonló előírások akár az MI kapcsán is relevánsak lehetnek (például: chatbottal vagy virtuális asszisztenssel folytatott beszélgetések megőrzése).

Jellemzőnek mondható továbbá, hogy ugyan a jogszabály nem írja elő kötelezően a személyes adatok megőrzését, azonban valamely jog gyakorlásához, illetve követelés érvényesítéséhez elévülési időt rendel. Például a magyar Polgári Törvénykönyvről szóló 2013. évi V. törvény 6:22. § (1) bekezdése értelmében a polgári jogi követelések – főszabályként – öt év alatt évülnek el. Magyarországon jellemzően ezen általános polgári jogi elévülési idő kerül figyelembevételére az esetleges érintetti követelésekkel vagy érintettek általi károkozásból származó követelésekkel szembeni védekezés kapcsán történő adatkezelések vonatkozásában, azonban az adott jogviszony, esetleges követelések, kapcsolódó eljárások sajátosságai szerint eltérő időtartamok figyelembevétele is releváns lehet. Természetesen erre tekintettel az is előfordulhat, hogy az idő múlása okán az adott személyes adat megőrzése már szükségtelenné válik, illetve, hogy maguk az adatok válnak irrelevánssá, amely esetben azokat az adatkezelő köteles törölni, illetve felismerhetetlenné tenni.[443] A fentieken túl olyan eset is felmerülhet, ahol jogszabály nem írja elő a személyes adatok kötelező megőrzését, illetve elévülési idő vagy jogorvoslatra irányadó egyéb időtartam sem vehető figyelembe. Ezen esetekben az adatkezelőnek az adatkezelés egyéb körülményeit, valamint az érintettek helyzetét, érdekeit és elvárásait is szükséges figyelembe vennie az adatmegőrzési idő meghatározásánál (például: az adott MI-rendszer alkalmazásával kapcsolatos körülmények, az adatok relevanciája a rendszer működése és fejlesztése kapcsán).

A fentieken túl – a hozzájáruláson alapuló adatkezelés esetén – a hozzájárulás érintett általi visszavonása egyben a hozzájárulás alapján kezelt személyes adatok törlését is szükségessé teszi. Így például, ha az érintett visszavonja a hozzájárulását ahhoz, hogy egy adott szolgáltató

[443] BUZÁS i. m. 220.

a részére nyújtott szolgáltatások személyre szabása kapcsán MI alapú megoldással vizsgálja az érintett preferenciáit, úgy az adatkezelő a fenti adatkezelés megszüntetése mellett köteles az érintett hozzájárulás alapján kezelt adatainak törlésére is. Ugyancsak köteles az adatkezelés megszüntetésére, valamint – eltérő jogszabályi, hatósági iránymutatás hiányában – a vonatkozó személyes adatok törlésére az adatkezelő, ha például az adatkezelő által alkalmazott MI alapú megoldás vagy az ennek révén végzett tevékenység adatkezelési művelet jogszabály-változásra vagy újabb hatósági gyakorlatra tekintettel tilossá válna. A fentebb írtak szerint azonban az adatok törlése helyett sor kerülhet azok anonimizálására is, az anonimizált adatokra – ha esetükben az érintettel való kapcsolat valóban visszaállíthatatlan módon megszüntetésre került –, ugyanis már nem vonatkoznak a személyes adatok védelmével kapcsolatos jogszabályi rendelkezések, így ezeket az adatkezelőknek már nem is szükséges figyelembe vennie.

Tekintettel az interneten keresztül történő adatkezeléseket jellemző nyilvánosságra, a GDPR előírja továbbá, hogy amennyiben az adatkezelő törölni köteles a személyes adatokat, amelyeket korábban nyilvánosságra hozott, az elérhető technológiát, illetve a megvalósítás költségeit is figyelembe véve köteles észszerű lépéseket tenni annak érdekében, hogy tájékoztassa a fenti adatokat kezelő egyéb adatkezelőket arról, hogy az érintett kérelmezte tőlük az ezen adatokra mutató linkek vagy az adatok másolatának törlését.[444] Mindez releváns lehet például abban az esetben, ha az érintett preferenciáit az érintett hozzájárulása alapján egy adott marketingszolgáltató bizonyos weboldalak üzemeltetőivel megosztja. Az érintett hozzájárulásának visszavonása esetén ezen szolgáltató köteles az adatok eltávolítása iránt intézkedni, ennek kapcsán technikai intézkedéseket tenni, illetve az adott weboldalak üzemeltetőit tájékoztatni az érintett törlése iránti kérelméről (amely ez esetben a hozzájárulás visszavonását is magában foglalja).

Az elfeledtetéshez való jog kapcsán – a GDPR vonatkozó követelményein túl – kiemelt jelentőséggel bír az EUB és az EJEB gyakorlata különösen a személyes adatok védelméhez való jog es a véleménynyilvánítás szabadságának ütközése kapcsán. Mivel egyik jog sem tekinthető abszolútnak, és alapvetően felelőséggel, észszerű korlátozások mellett gyakorolhatók az online világban is, igy ezen esetekben lényegében esetről-esetre vizsgálandó, hogy az érdekek összemérése melyik jog érvényesüléséhez vezethet.[445] Még a GDPR

[444] GDPR 17. cikk (2) bek.
[445] SCHUBAUER Petra: Az elfeledtetéshez való jog az új Adatvédelmi Rendelet tükrében. *Infokommunikáció és jog*, 2017/2. 88.

alkalmazását megelőzően született meg 2014-ben a döntés az ún. Google Spain ügyben, amelyben az EUB lefektette az elfeledtetéshez való jog kereteit. Az ügy során González egy számára hátrányos, őt említő korábbi cikk kapcsán kérte a nevére mutató találatok eltávolítását a Google keresési találatai közül. Az EUB az ügy kapcsán hangsúlyozta, miszerint az érintett jogainak védelmét nem lehetne hatékonyan biztosítani, ha a keresőszolgáltatók helyett az érintettnek először vagy egyidejűleg az adott honlap szerkesztőjéhez kellene fordulniuk,[446] emellett eltérő jogos érdekek állhatnak fenn a keresőmotor működtetője és a weboldal szerkesztője által végzett adatkezelések tekintetében.[447] Hangsúlyozandó, hogy az EUB mellett az EJEB is több ízben foglalkozott az elfeledtetéshez való joggal. A Biancardi v. Olaszország ügyben az EJEB egy olasz bírósági döntést vizsgált, amely egy olasz lap kiadójának felelősségét állapította meg egy korábbi, étteremben történt verekedésről, vonatkozó büntetőügyről tudósító cikk interneten való további elérhetősége kapcsán, továbbá sérelemdíj megfizetésére, valamint költségek viselésére kötelezte. Az eset során az EJEB nem állapította meg a véleménynyilvánítás szabadságának elsőbbségét, továbbá különös jelentőséget tulajdonított annak a körülménynek, hogy a vonatkozó cikk nem politikusról vagy más közszereplőről szólt, annak hosszabb időn keresztüli elérhetővé tétele pedig aránytalan mértékű kárt okozott az érintettnek.[448] A fentiekben az EJEB egyben vissza is utal a korábbi Axel Springer AG v. Németország ügyre,[449] amelyben az EJEB egy ismert németországi tévészínész letartóztatásáról való tudósítással kapcsolatos eset vonatkozásában döntött, hangsúlyozva az információ közzétételével kapcsolatos érdek és az érintett magánélete védelméhez fűződő jogának összemérését, valamint az érintett közszereplő mivoltát, az üggyel kapcsolatos közérdeklődést.[450] Adatvédelmi szempontból tehát jelentős különbség van a között, ha a közszereplők, illetve egyéb – főként közéleti szempontból jelentős tevékenységet nem végző, illetve a közügyek vitatásában részt nem vevő – személyek adatainak kezelése történik.[451] A véleménynyilvánítás szabadságával és a személyes adatok védelmével kapcsolatos alapjogi ütközést ennek tükrében ugyanúgy el kell végezni olyan esetekben is, ha az adott tartalmat MI-rendszer segítségével hozták létre (például: MI által alkotott cikkek vagy chatbot által a nagyközönség számára adott válaszok esetén), amely esetekben a vonatkozó tartalmak által

[446] C-131/12. sz. ügy Google Spain SL, a Google Inc. és az Agencia Española de Protección de Datos, Mario Costeja González között folyamatban lévő eljárásban [ECLI:EU:C:2014:317] 82. pontja
[447] C-131/12. sz. ügy, 86. pontja
[448] Biancardi v. Italy, no. 77419/16., 2021. november 25-i ítélet, 62. bek.
[449] Biancardi v. Italy, 61-63. bekezdések
[450] Axel Springer AG v. Germany, no. 39954/08., 2012. február 7-i ítélet, 106–107. bekezdések
[451] KOLTAY András: *Freedom of Speech. The Unreachable Mirage*. Budapest, Complex Publisher Ltd., 2013. 245.

említett személyek státusza, tevékenysége, valamint a vonatkozó megnyilvánulás tényállítás, illetve ténybeli alappal rendelkező vélemény vagy szubjektív értékítélet jellege vélhetően jelentőséggel bírna.[452]

A Hurbain v. Franciaország ügyben az EJEB újfent a véleménynyilvánítás szabadságát vette össze a személyes adatok védelmével, illetve az elfeledtetéshez való joggal. Az ügyben egy franciaországi kiadót kötelezett a nemzeti bíróság egy online cikk anonimizálására, amely egy közel húsz évvel korábbi halálos balesetről számolt be, annak további közzététele pedig a korábbi elkövető személyes adatok védelméhez fűződő jogát sértette. Az eset során az EJEB arra a következtetésre jutott, hogy az anonimizálásra kötelezés kapcsán az illetékes bíróság helyesen vetette össze a véleménynyilvánítás szabadságát a személyes adatok védelmével, és jutott arra a következtetésre, hogy a döntés nem sérti a véleménynyilvánítás szabadságát. Ennek során kiemelte, miszerint a cikk további online elérhetővé tétele egyfajta „virtuális bűnügyi nyilvántartás" létrejöttét eredményezte az érintett vonatkozásában.[453] Emellett az ítélet kiemeli, miszerint az a sajtót az őt megillető jogok mellett megfelelő kötelezettségek és korlátozások is terhelik, amelynek szükséges alávetnie magát, a vonatkozó, elavult információt hordozó cikkek anonimizálása pedig ezek körébe helyezkedik.[454] Ennek kapcsán megjegyzendő azonban, hogy a Big Data korában az anonimizálás sem lehet minden esetben tökéletes megoldás, és akár statisztikai adatok alapján is azonosíthatók lehetnek érintettek,[455] mindezt adott esetben a médiatartalom-szolgáltatóknak is figyelembe kell venniük munkájuk során.

Az MI-modellek kapcsán az érintett személyes adatainak törlése, illetve az érintett azonosíthatóságának megszüntetése érdekében sor kerülhet maga a modell, vagy az ahhoz kapcsolódó, illetve az által alapul vett információk (például: tanítóadatok) törlésére. E körbe tartozhat adott esetben a tanítóadatok „tisztítása" is, amely során a modell implementálásához és további felhasználásához szükségtelen adatok eltávolításra kerülnek.[456] Emellett végső esetben sor kerülhet a modell törlésére is. Az adott modell törlése a jogsértő adatkezelés megszüntetése mellett adott esetben a korábbi sérelmek egyfajta orvoslásaként is szolgálhat.[457]

[452] KOLTAY András: A véleményszabadság alkotmányos védelme az Alaptörvény első évtizedében. *Acta Humana*, 2021/2. 71.
[453] Hubarlain v. Belgium, no. 57292/16., 2023. július 4-i ítélet, 255–257 bekezdések
[454] Hubarlain v. Belgium, 177. és 244. bekezdések
[455] KESERŰ Barna Arnold: *A 21. századi technológiai változások hatása a jogalkotásra. Képes-e lépést tartani a jog a változó világgal?*, Budapest, Dialóg Campus Kiadó, 2020. 22.
[456] AEPD GDPR Compliance Introduction, 24.
[457] Jevan HUTSON, Ben WINTERS: America's Next 'Stop Model!': Model Deletion. *Georgetown Law Technology Review*, vol. 8. no. 1. (January 2024). 131.

A gyakorlatban ugyancsak alkalmazhatók az ún. „*model disgorgement*” megoldások, amelyek nem csak magukat az adatokat, hanem azok érintettre gyakorolt hatásait is megszüntetik,[458] valamint az ún. gépi elfelejtési (angolul: „*machine unlearning*”) technikák is. A fentiek körébe olyan megoldások, eljárások tartoznak, amelynek eredménye az érintettre vonatkozó információk MI általi törlése, így tulajdonképpen az MI általi „elfelejtésre” kerül sor a teljes modell újra tanítása nélkül.[459] A generatív MI alkalmazások esetén különös kihívást jelenthet továbbá a fejlesztéshez használt tanítóadatok kikövetkeztetése a modellből (angolul: „*model inversion*”), valamint az adatszivárgással kapcsolatos kockázatok, amelyek adott esetben megkérdőjelezhetik az érintettre vonatkozó információk törlésének, valamint az MI által használt adatok és az érintett közötti kapcsolat megszüntetésének sikerességét.[460]

Kiemelendő, hogy a törléshez való jog kapcsán is beszélhetünk kivételekről, amelyek esetén ezen jog nem gyakorolható, ideértve azon eseteket, amennyiben az adatkezelésre

- a véleménynyilvánítás szabadságához, illetve a tájékoztatáshoz való jog gyakorlása érdekében,
- az adatkezelőre irányadó jogi kötelezettség teljesítése, illetve közhatalom gyakorlása, közérdek érvényesítése érdekében,
- népegészségügyi területet érintő közérdek alapján,
- közérdekű archiválás céljából, illetve tudományos és történelmi kutatási célból vagy statisztikai célból, vagy
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges körben kerül sor.[461]

Így amennyiben például egy kontaktszemély felkutatására egy MI megoldás alkalmazásával kerül sor, úgy – a vonatkozó jogszabályi rendelkezésekre tekintettel – ennek kapcsán a népegészségügyi érdek az adatkezelés vonatkozásában mindaddig hivatkozható lehet, amíg ezen kontaktszemély azonosítása szükséges. Ugyancsak hivatkozható lehet a jogi igények védelme érdekében való adatkezelés szükségessége, ha az adatkezelő az érintett virtuális asszisztenssel folytatott beszélgetését kívánja megőrizni, mindaddig, amíg az érintett reálisan

[458] Alessandro ACHILLE, Michael KEARNS, Carson KLINGENBERG, Stefano SOATTO: *AI Model Disgorgement: Methods and Choices*, 2023.04.07, arXiv:2304.03545v1, https://doi.org/10.48550/arXiv.2304.03545. 1.
[459] Tom SIMONITE: Now That Machines Can Learn, Can They Unlearn?, *Wired*, 2021.08.19, https://www.wired.com/story/machines-can-learn-can-they-unlearn/
[460] NOVELLI, CASOLARI, HACKER, SPEDICATO, FLORIDI op. cit. 12.
[461] GDPR 35. cikk (1) bek.

követelést érvényesíthet az adatkezelővel szemben (például egy vitás helyzetben). Hangsúlyozandó azonban, hogy a fenti kivétel-szabályok korlátlanul vagy pusztán általános hivatkozásként nem alkalmazhatók. Így tehát például egy arcfelismerő rendszert alkalmazó adatkezelő nem figyelheti folyamatos jelleggel az irodahelyisége teljes területét (és így az ott tartózkodó munkavállalókat, látogatókat) arra hivatkozással, hogy a technológia alkalmazása, illetve az ezzel kapcsolatos információk megőrzése egy esetleges betörés esetén az elkövető könnyebb azonosítását segítheti. Megjegyzendő azonban, hogy bár a fenti kivételek kevéssé hivatkozhatók e körben, ám – különösen általános célú MI-modellek esetén – az érintett törléshez való vagy egyéb adatvédelmi jogának (például: korlátozáshoz való jog) gyakorlása akadályokba ütközhet a személyes adatok tanítóadatok közül való eltávolítása kapcsán, ugyanis egy ilyen kérelem teljesítéséhez az adat kimenetekre gyakorolt hatásait vagy magát a vonatkozó algoritmust kellene törölni, amely a gyakorlatban kevéssé tűnik életszerű megoldásnak.[462]

iii. Az adatkezelés korlátozásához való jog

Az MI kapcsán szintén érdemes az adatkezelés korlátozásához való jogról beszélni, ugyanis az MI és a kapcsolódó technológiai környezet sajátosságai okán ennek a jognak a gyakorlása esetén is különös szempontok érvényesülnek.

Adatkezelés korlátázásra (vagy másként szólva az adatok zárolására) az érintettnek abban az esetben van lehetősége, amennyiben

- az érintett vitatja az adatok pontosságát; ez esetben a korlátozás az adatok pontosságának tisztázásáig, ellenőrzéséig tart,
- az adatkezelés jogellenes, az érintett azonban az adatok törlése helyett azok felhasználásának korlátozását kéri,
- az adatkezelőnek ugyan már nincs szüksége az adatokra az adatkezelés céljából, azonban az érintett azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kéri,
- az érintett tiltakozott az adatkezelés ellen; ez esetben az adatkezelői jogos érdek elsőbbségének megállapításáig tart az adatkezelés korlátozása.[463]

[462] WOLFF, LEHR, YOO op. cit. 22.
[463] GDPR 18. cikk

A gyakorlatban az adatkezelés korlátozása, illetve az adatok zárolása többféle módon is megvalósítható, így például sor kerülhet arra a személyes adatokat tartalmazó adatbázishoz kapcsolódó hozzáférési jogok felfüggesztésével vagy honlapon elérhető adatok ideiglenes eltávolítása útján.[464] Az érintett különösen jogosult lehet az adatok zárolását kérni, ha pontatlan adatok kerültek rögzítésre (például: tévesen azonosított ügyfél, hibásan feljegyzett kapcsolattartási adatok), amely esetben az adatkezelő mindaddig köteles az adatok zárolása iránt intézkedni, amíg az adatok pontossága nem tisztázható. Az MI esetén azonban ezen jog gyakorlása kérdésesen foghat helyt, tekintettel arra, hogy adott esetben a pontatlan vagy hibás adat is jelentőséggel bírhat az MI tanulási folyamata, illetve a későbbi hibák elkerülése szempontjából.[465] Így ezen jog gyakorlása jellemzően emberi ügyintéző segítségével foghat helyt (például: ügyféladatok kiigazítása, amelyeket az MI alapul vehet virtuális asszisztensi támogatás során), vagy bizonyos esetekben akár az adott MI megoldás igénybevétele útján, a felhasználási folyamat részeként is támogatható. Így például maga a virtuális asszisztens is intézkedhet az egyszerűen és gyorsan teljesíthető érintetti kérelmek, köztük adott esetben egyes adatkezelés korlátozása iránti kérelmek kapcsán, míg az összetettebb vagy komplexebb felülvizsgálatot igénylő ügyekben egy emberi ügyintézőnek továbbíthatja a kérelmet. Az adott alkalmazás így például egy könnyen azonosítható pontatlan adatot maga is azonosíthat, és zárolhat a kérelem elbírálásáig, vagy ha az adott kérelem rögtön elbírálható, úgy maga is kijavíthatja a pontatlan adatokat. Ennek kapcsán azonban hangsúlyozandó, hogy a fentiek kapcsán csak olyan kérelmek elbírálásában vehet részt az MI, amelyeket képes az irányadó jogszabályokkal összhangban, illetve megfelelő hatékonysággal kezelni. Mindaddig, amíg erre az MI bizonyíthatóan nem képes, szükséges emberi ügyintéző bevonása az adott kérelem elbírálása kapcsán. Megjegyzendő azonban, hogy az adott MI megoldás az emberi ügyintéző közreműködéséig is képes lehet arra, hogy például az érintett által pontatlannak vagy jogellenesen kezeltnek jelölt adatokat zárolja, és az adott ügyintéző felé továbbítsa az érintett kérelmét, illetve segítsen az emberi ügyintézővel való kapcsolatteremtésben a kérelem mielőbbi elbírálása érdekében.

Az adatkezelés korlátozásához való jog kapcsán ugyancsak fontosnak tekinthető kiemelnünk, hogy az adatok zárolása esetén azoknak jellemzően el kell különülniük a további, zárolás által nem érintett adatoktól. Így tehát azokat az adatkezelőnek egyértelműen meg kell jelölnie, vagy külön adathordozóra, illetve erre a célra szolgáló adatbázisba kell áthelyeznie. Mindennek célja

[464] BUZÁS i. m. 233.
[465] Lásd: NECZ (2022b) i. m. 108.

az adatkezelés felfüggesztése az adott adat vonatkozásában az érintetti kérelem teljesítéséig, illetve annak tisztázásáig. Mindez az MI esetén problémákba ütközhet, hiszen míg az MI képes lehet azonosítani a „problémás" adatokat, azok „aktív" adatkészletből való eltávolítása számos esetben kérdésesen valósítható csak meg, hiszen a vonatkozó adatok szükségesek lehetnek például az adott megoldás hatékony működtetéséhez. Ehhez adott esetben azonban a fentebb, a törléshez való jog kapcsán ismertetett technikák, megoldások is alkalmazhatók lehetnek, így, ha ez az adott esteben lehetséges, valamennyi, az adott érintettre vonatkozó összefüggés eltávolítható, illetve adatkezelési művelet megszüntethető az adatkezelés korlátozásának időtartama alatt.

Szintén szokatlan helyzet állhat elő azokban az esetekben, ahol az adatkezelőnek már nincs szüksége az MI alapú adatkezelések kapcsán egy bizonyos adatra, az érintett azonban igényli azt, például jogi igények előterjesztéséhez vagy védelméhez. Erre példaként szolgálhat egy arcfelismerő rendszerrel ellátott kamera által rögzített felvétel. Az adatkezelési idő lejárta előtt benyújtott érintetti kérelem alapján az adatkezelő például köteles lehet ezen felvétel és az érintett azonosítására vonatkozó további információk további, zárolt kezelésére az érintettnek vagy hatóságoknak történő kiadásig, egy ilyen felvétel és a kapcsolódó információk segíthetik ugyanis annak alátámasztását, hogy az érintett adott időpontban hol tartózkodott.

iv. Az adathordozhatósághoz való jog

Az adathordozhatósághoz való jog keretében az érintett jogosult arra, hogy személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja, illetve, hogy adatai másik adatkezelőnek való, akár közvetlen továbbítását is kérje.[466] Így például, ha az érintett egy hírközlési szolgáltató ügyfele, úgy szolgáltatóváltás esetén kérheti egyes, hírközlési szolgáltatás igénybevételével kapcsolatosan automatizált módon kezelt adatai továbbítását az új szolgáltatónak. A fentiekre tekintettel pedig az adathordozhatósághoz való jog akár a hozzáféréshez való jog egyfajta kiegészítéseként is tekinthető, azonban az adatkezelés ellenőrzésén túl ezen jog az érintett információs önrendelkezési jogának érvényesítését is szolgálja.[467] Hangsúlyozandó azonban, hogy e tekintetben is lehetnek korlátozások, amely esetekben ezen jog nem gyakorolható, ideértve különösen, amennyiben az adattovábbításnak

[466] GDPR 20. cikk (1)-(2) bekezdései
[467] BUZÁS i. m. 205.

technikai akadálya merülne fel.[468] Így például, amennyiben az adatkezelő olyan technikai megoldást vagy eljárást alkalmaz, amelynek hasonló alkalmazása a másik potenciális adatkezelőnél nem biztosítható, úgy ez adott esetben akadályozhatja az adathordozhatósághoz való jog gyakorlását.

A gyakorlatban ugyancsak problémát jelenthet e körben, amennyiben a továbbításhoz üzleti titok vagy szellemi tulajdon által védett megoldás versenytársnak való felfedése válna szükségessé (például: forráskód felfedésének szükségessége merülne fel). Ezen helyzet jellemzően az érintett személyes adatok védelméhez fűződő jogának, valamint az adatkezelő szellemi alkotások védelméhez fűződő, elsősorban vagyoni érdekeinek ütközéséhez vezethet, amely az adott eset lényeges körülményeinek figyelembevételével oldható csak fel. Amennyiben például az érintett olyan adatai továbbítását kéri egy másik adatkezelőnek, amelyekhez üzleti titok vagy más nem nyilvános oltalom, ismeret felfedése szükséges, úgy az adatkezelő szellemi tulajdon védelmével kapcsolatos érdekei ennek kapcsán adott esetben az érintetti érdekeknél erősebbek lehetnek, különösen akkor, ha például kulcsfontosságú szellemi tulajdon felfedése válna szükségessé versenytárs számára, vagy az adattovábbítás megszervezése aránytalan teherrel, indokolatlan költségekkel járna. Ilyen esetekben az adatkezelői érdek elsőbbségét, illetve a kérelem teljesíthetőségének akadályát azonban vita esetén az adatkezelőnek szükséges bizonyítania. Adott esetben továbbá az érintett kérelme akár a fenti információk kitakarásával is teljesíthető.[469] Így például az adatkezelőknek általában nem szükséges MI általi adatkezelés esetén sem felfedniük üzleti titkaikat a versenytársak számára az adathordozhatósághoz kapcsolódó kérelmek teljesítése érdekében, azonban elvárható lehet, hogy az MI által kezelt érintettre vonatkozó adatokat olyan módon továbbítsák, amelyek révén így a fogadó fél is képes azokat feldolgozni (például: banki, telekommunikációs szolgáltatók esetén, a vonatkozó jogszabályi rendelkezésekkel összhangban). Kiemelendő továbbá, hogy az adathordozhatósághoz való jog gyakorlására tekintettel rendelkezésre bocsátandó személyes adatokat széles körben használt, géppel olvasható formátumban szükséges rendelkezésre bocsátani, amelyek körébe jellemzően az ismert, széles körben, akár ingyenesen is elérhető fájlformátumok tartoznak, az adatok kinyerését korlátozó vagy lehetetlenné tevő megoldások azonban nem tartoznak e körbe, azok az adathordozhatósághoz való jog gyakorlását meggátolhatják.[470]

[468] GDPR 20. cikk (2) bek.
[469] NECZ (2022b) i. m. 109–110.
[470] BUZÁS i. m. 207.

Hangsúlyozandó továbbá, hogy ezen jog csak azon esetekben gyakorolható, amikor az adatkezelés az érintett hozzájárulásán vagy a közvetlenül vele kötött szerződésen alapul és az adatkezelés automatizált módon történik.[471] Így tehát, amennyiben az érintett egy virtuális asszisztenst vagy chatbot alkalmazást vesz igénybe, úgy ezen jog – elméletileg – gyakorolható, míg ha az érintettet foglalkoztató gazdasági társaság szerződik a szolgáltatóval, és az érintett ezen megállapodás, illetve az ehhez kapcsolódó szerződéses kommunikáció keretein belül használja a virtuális asszisztens vagy chatbot alkalmazást, úgy az adathordozhatósághoz való jog gyakorlása a GPDR alapján már kérdésesen foghat helyt, hiszen ez esetben az adatkezelés az érintettet foglalkoztató gazdasági társaság jogos gazdasági érdekéhez kapcsolódik. Nem alkalmazandó továbbá ezen jog azon estekben, amennyiben az adatkezelő közérdekű adatkezelést végez, vagy az adatok kezelését a rá ruházott közhatalmi jogosítvány keretein belül végzi.[472] E körbe tartozhatnak például az egyes bűnüldöző szervek által használt MI-alkalmazások, hatóságok általi közterületen folytatott megfigyelés. A fentieken túl megemlítendő, hogy az érintett adathordozhatósághoz való joga nem érintheti hátrányosan mások jogait és szabadságait sem.[473] Így például ezen jog gyakorlása nem eredményezheti egyúttal olyan érintettek adatainak átadását egy másik adatkezelő részére, akik adott esetben erről nem bírnak tudomással, vagy akik ezzel kapcsolatban nem adták hozzájárulásukat, vagy esetükben ennek kapcsán más jogalap megléte nem igazolható.

Hangsúlyozandó, hogy a GDPR rendelkezésein túl egyéb jogszabályok is lehetőséget biztosíthatnak az érintettek számára bizonyos információkhoz való hozzáférésre, valamint ezek más szolgáltatóknak történő továbbítására. E körbe tartozhat például az európai adatrendelet („**Adatrendelet**”)[474] keretein belül a termékadatoknak[475] és kapcsolódószolgáltatás-

[471] GDPR 20. cikk (1) bek.
[472] GDPR 20. cikk (3) bek.
[473] GDPR 20. cikk (4) bek.
[474] Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet), PE/49/2023/REV/1, HL L, 2023/2854, 2023.12.22, ELI: http://data.europa.eu/eli/reg/2023/2854/oj (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV).
[475] Adatrendelet 2. cikk 16. pontja értelmében termékadatok: „*egy összekapcsolt termék használata által generált olyan adatok, amelyeket a gyártó úgy tervezett, hogy a felhasználó, az adatbirtokos vagy egy harmadik fél – beleértve adott esetben a gyártót is – elektronikus hírközlési szolgáltatás, fizikai kapcsolat vagy eszközön való hozzáférés révén visszanyerhesse azokat*”.

adatoknak[476] az összekapcsolt termékek[477] vagy kapcsolódó szolgáltatások[478] felhasználói részére történő rendelkezésre bocsátása, adattovábbítások biztosítása,[479] amely adott esetben kiegészíti az érintettek hozzáférési, illetve adathordozhatósághoz való jogának gyakorlását a GDPR alatt.[480] Ennek tükrében az olyan esetekben, amikor a felhasználó nem tud az összekapcsolt termékből vagy a kapcsolódó szolgáltatásból közvetlenül hozzáférni az adatokhoz, az adatbirtokosnak a felhasználó kérelmére indokolatlan késedelem nélkül könnyen elérhető adatokat, valamint az ezek értelmezéséhez és felhasználásához szükséges releváns metaadatokat szükséges hozzáférhetővé tennie számára.[481] Ennek kapcsán azonban az Adatrendelet kiemeli, miszerint a felhasználó nem élhet vissza az adatbirtokos technikai infrastruktúrájának hiányosságaival az adatokhoz való hozzáférés érdekében.[482] A hozzáférés biztosításán túl a felhasználó kérelmére továbbá az adatbirtokosnak könnyen hozzáférhető adatokat, illetve a releváns metaadatokat harmadik fél (például a felhasználó számára további szolgáltatásokat nyújtó vállalkozás) rendelkezésére kell bocsátania – adott esetben és amennyiben ez technikailag kivitelezhető – folyamatosan és valós időben.[483] Megjegyzendő, hogy ezen harmadik fél a továbbított adatokat – ha ez a felhasználónak történő szolgáltatás nyújtásához nem szükséges – nem használhatja fel a profilalkotásra.[484] Így például ezen további szolgáltató a kapott adatokat nem vizsgálhatja algoritmusokkal annak érdekében, hogy a felhasználót vásárlói csoportba sorolja, és a részére ennek megfelelő termékeket jelenítsen meg.

Kiemelendő továbbá, hogy az Adatrendeletben biztosított adathozzáférési jogok kiterjednek a virtuális asszisztensekre is, amennyiben azok interakciót folytatnak egy összekapcsolt

---

[476] Adatrendelet 2. cikk 16. pontja értelmében kapcsolódószolgáltatás-adatok: „*olyan, az összekapcsolt termékhez kapcsolódó felhasználói műveletek vagy események digitalizálását képviselő, valamely kapcsolódó szolgáltatás szolgáltató általi nyújtása során a felhasználó által szándékosan rögzített vagy a felhasználói művelet mellékterméke*ként generált adatok".

[477] Adatrendelet 2. cikk 5. pontja értelmében az összekapcsolt termék: „*olyan tárgy, amely a felhasználására vagy a környezetére vonatkozó adatokat szerez meg, generál vagy gyűjt, és amely elektronikus hírközlési szolgáltatáson, fizikai kapcsolaton, vagy eszközön való hozzáférésen keresztül képes termékadatokat közölni, és amelynek elsődleges funkciója nem az adatoknak a felhasználótól eltérő bármely más fél nevében történő tárolása, kezelése vagy továbbítása*".

[478] Adatrendelet 2. cikk 6. pontja értelmében a kapcsolódó szolgáltatás: „*olyan, az elektronikus hírközlési szolgáltatásoktól eltérő digitális szolgáltatás, a szoftvert is beleértve, amely a vásárláskor, bérléskor vagy lízingeléskor össze van kapcsolva a termékkel oly módon, hogy a hiánya lehetetlenné tenné az összekapcsolt termék egy vagy több funkciójának ellátását, vagy amelyet a gyártó vagy egy harmadik fél utólag kapcsol össze a termékkel, hogy kiegészítse, frissítse vagy módosítsa az összekapcsolt termék funkcióit*".

[479] Adatrendelet 1. cikk (1) bek.

[480] Adatrendelet 1. cikk (5) bek.

[481] Adatrendelet 4. cikk (1) bek.

[482] Adatrendelet 4. cikk (11) bek.

[483] Adatrendelet 5. cikk (1) bek.

[484] Adatrendelet 6. cikk (2) bek. (p) pontja

termékkel vagy kapcsolódó szolgáltatással.[485] Mindez azonban csak a felhasználó és az összekapcsolt termék vagy kapcsolódó szolgáltatás közötti, virtuális asszisztensen keresztüli interakcióból származó adatokra vonatkozik, ugyanis az Adatrendelet szerinti adathozzáférési jogok nem gyakorolhatók a fentiek körén kívül eső interakciókra és az annak során generált vagy egyébként kezelt adatokra vonatkozóan.[486]

Habár az Adatrendelet szerinti hozzáférési és adathordozhatósághoz való jogok megkönnyíthetik és támogathatják a felhasználók információs önrendelkezési jogának gyakorlását, hatékonyságuk – különösen a GDPR viszonylatában – megkérdőjelezhető lehet, különösen ideértve az Adatrendelet szerinti adathordozhatósághoz való jogot, amelynek GDPR által biztosított adatvédelmi megfelelője is a gyakorlatban az egyik legritkábban hivatkozott jognak tekinthető.[487] Megemlítendő továbbá, hogy bár a fenti hozzáférési, illetve adathordozhatósághoz való jog ugyan kétségtelenül további rendelkezési jogokat biztosít az érintetteknek adataik felett, a fentebb írt szempontokon túl is kérdéses, hogy ezzel az érintettek a gyakorlatban milyen mértékben fognak élni, tekintettel például az eltérő szolgáltatások ismeretének hiányára, valamint az adott megoldás vagy platform felhasználó általi „megszokására".[488]

v. A tiltakozáshoz való jog

Az érintett tiltakozáshoz való joga a közérdekű, illetve közhatalmi jogosítvány gyakorlásának körébe tartozó, valamint a jogos érdek alapján végzett adatkezelések esetén bír relevanciával, e körbe értve a profilalkotást is.[489] A tiltakozás joga értelemszerűen szemben áll az adatkezelő érdekeivel, így ilyen esetekben az adatkezelés csak akkor folytatható, ha az adatkezelő bizonyítja, hogy az általa az adatkezelés alapjaként hivatkozott jogos okok elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben.[490] Ezt az adatkezelőnek az érdekmérlegelési tesztben szükséges kifejtenie és alátámasztania, az érintetti és az adatkezelői érdekek egyértelmű azonosításával és összemérésével, amelynek összefoglalásaként az

[485] Adatrendelet 1. cikk (4) bek.
[486] Adatrendelet (23) preambulum-bekezdés
[487] Wolfgang KERBER: Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. *GRUR International*, vol. 72., issue 2. (2023) 125.
[488] Gintaré SURBLYTÉ: Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy. *GRUR International*, vol. 65., issue 12. (2016) 1125.
[489] GDPR 21. cikk (1) bek.
[490] Uo.

adatkezelő vagy harmadik fél jogos érdekeit az adatvédelmi tájékoztatóban is szükséges megjeleníteni.[491] A fentiekre tekintettel MI általi adatkezelés esetén például az érdekmérlegelési tesztben kifejthetők az adott MI-rendszer, valamint annak alkalmazása társadalmi hasznosságával kapcsolatos okok is (például: kutatási célú felhasználások, e célból alkalmazott rendszerek esetén). Megemlítendő ugyanakkor, hogy a tiltakozáshoz való jog nem értelmezhető kiterjesztően, így az az egyéb jogalapok vonatkozásában nem, kizárólag a közérdekű, illetve jogos érdeken alapuló adatkezelések esetén gyakorolható.[492]

Amennyiben a személyes adatok kezelésére üzletszerzés érdekében került sor, úgy az érintett tiltakozását az adatkezelőnek tiszteletben kell tartania és meg kell szüntetnie az adatkezelést; e tekintetben ugyanis az adatkezelői érdek nem élvezhet elsőbbséget az érintett érdekeivel szemben.[493] Így tehát, amennyiben az érintett részére az adatkezelő a fennálló ügyfélkapcsolatra, valamint az érintett által korábban igénybe vett szolgáltatásokra tekintettel küld direkt marketing üzenetet, úgy az érintett tiltakozását az adatkezelő köteles figyelembe venni, és a továbbiakban az adatkezelés folytatásától eltekinteni. Hangsúlyozandó azonban, hogy az üzleti célú adatkezelések egyéb esetei is jelentős részben az adatkezelő jogos érdekén alapulnak, különösen ideértve az üzletfejlesztési célú adatfelhasználásokat (például adott esetben az önvezető autó egyes funkcióinak használata, fejlesztése céljából a vezetési és utasinformációk kezelése).[494]

Az MI általi adatkezelés esetén a tiltakozáshoz való jog a felhasználói adatoknak a gépi tanulás céljára történő felhasználása kapcsán is felmerülhet. E körben megoldást jelenthet például a nagy nyelvi modellek szolgáltatói általi tiltakozási jog („*opt-out right*") biztosítása, illetve különböző gépi elfelejtési (*machine unlearning*) megoldások implementálása.[495] A fenti megoldások segítségül szolgálhatnak az érintettek személyes adatainak védelméhez anélkül, hogy a különböző MI megoldásokat alkalmazó szolgáltatók gazdasági érdekeit jelentős mértékben sértenék, illetve az MI-rendszerek, illetve modellek fejlesztését aránytalanul akadályoznák. A személyes adat érintetthez való kapcsolatának eseti, kontextuális jellege, valamint az érintett újbóli azonosíthatóságával kapcsolatos kihívások okán – az érintett

[491] GDPR 13. cikk (1) d) pontja, 14. cikk (2) b) pontja
[492] BUZÁS i. m. 240.
[493] GDPR 21. cikk (2)-(3) bekezdései
[494] AI Discussion paper, Baden-Württemberg VI. 1. (1).
[495] NOVELLI, CASOLARI, HACKER, SPEDICATO, FLORIDI op. cit. 15.

elfeledtetéshez való joga kapcsán fentebb írtakra tekintettel – azonban kérdéses lehet, hogy adott esetben az érintett MI általi elfelejtése ténylegesen milyen mértékben garantálható.

Kiemelendő, hogy a tiltakozáshoz való jog tudományos és történelmi kutatási célú, valamint statisztikai célú adatkezelés esetén is releváns lehet, és ezen esetekben is gyakorolható az érintett saját helyzetével kapcsolatos okokból, ide nem értve azt az esetet, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében kerül sor.[496] Így amennyiben egy adott hatóság közérdekű feladatai körében gyűjt statisztikai adatokat az érintettről MI-rendszer támogatásával, úgy e körben az érintett tiltakozása jellemzően nem foghat helyt.

Az adatok tanítási célú felhasználásával szembeni tiltakozást az egyes MI-rendszerek szolgáltatói jellemzően a vonatkozó alkalmazáson, weboldalon belül biztosítják a felhasználók számára. Kérdéses azonban, hogyan gyakorolható a tiltakozáshoz való jog például MI-modellek fejlesztői, egyes (jellemzően általános célú) MI-rendszerek szolgáltatói általi adatbányászat esetén, ahol az interneten nyilvánosan elérhető információkat gyűjtenek a modell tanításához, illetve az adott rendszer működtetéséhez (például: az interneten való keresés a felhasználói kérdésekre adott válasz megfogalmazása céljából), amelyek sok esetben az adatkezelővel kapcsolatban nem álló személyekre vonatkozó személyes adatokat is tartalmaznak. Habar ezen gyakorlat adatvédelmi megítélésé kétségtelenül vitatott, mégis számos szolgáltató él ezzel a lehetőséggel. Ennek tükrében megemlítendő, hogy a digitális egységes piacon a szerzői és szomszédos jogokról szóló irányelvben ("**CDSM Irányelv**") meghatározott, a szerzői jogi oltalom alá eső művek kapcsán alkalmazott szöveg- és adatbányászat alóli kívülmaradás joga[497] kizárólag ezen oltalom alá eső művek jogosultjai által hivatkozható, a személyes adatok védelme kapcsán azonban nem találunk ilyen speciális rendelkezést, igy – az irányadó jogalap függvényében – az érintettek a hozzájárulás megtagadására vagy visszavonására, illetve a tiltakozáshoz való jog gyakorlására hivatkozhatnak. Megemlítendő továbbá, hogy a CDSM Irányelv fenti rendelkezése kifejezetten nevesíti a művek és más védelem alatt álló teljesítmények felhasználásának „*például az interneten keresztül nyilvánosan hozzáférhetővé tett tartalom esetében géppel olvasható módszerek révén*" való kizárását. Erre a gyakorlatban egységes megoldás még nem alakult ki,

[496] GDPR 21. cikk (6) bek.
[497] Lásd: Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, 4. cikk (3) bek.

elterjedtnek számít azonban például a webböngészők számára utasítást adó robots.txt. kiterjesztés vagy a Spawning nevű nemet közösségi kezdeményezéshez köthető ai.txt. kiterjesztés alkalmazása.[498] Kérdéses azonban, hogy hasonló megoldások elterjednek-e majd a személyes adatok védelme, illetve a tiltakozáshoz való jog gyakorlása területén is. Ennek kapcsán megjegyezzük továbbá, hogy az olasz adatvédelmi hatóság 2023. végén széleskörű hatósági vizsgalatot indított annak megállapítása érdekében, hogy a köz-, illetve magánszférába tartozó szervezetek weboldalain alkalmazott beállítások megfelelően védik-e a felhasználók jogait a web scraping tevékenységgel szemben.[499] Ennek tükrében előfordulhat, hogy a web scraping tevékenységgel szembeni tiltakozás lehetősége mellett a web scrapinggel szembeni védekezés a weboldalakat üzemeltető adatkezelők oldaláról adatbiztonsági kötelezettsége is alakul.

vi. Az automatizált döntéshozatal és a profilalkotás

A fentieken túl továbbá különös gonddal vizsgálandó az MI alkalmazása az automatizált döntéshozatallal, különösen profilalkotással kapcsolatos adatkezelések esetén, ideértve kiváltképp azokat az eseteket, ahol a fentiek szerinti adatkezelések eredményeként hozott döntés hatása az érintettre nézve joghatással járna, vagy őt ehhez hasonlóan jelentős mértékben érintené.[500] Ilyen esetekben értelemszerűen az MI alkalmazása különösen a fogyasztói akarat manipulálásához, eltorzításához, valamint negatív társadalmi és gazdasági hatásokhoz, következményekhez vezethet. Megemlítendő ennek kapcsán, hogy az MI alkalmazását szükséges elkülönítenünk az egyes döntéshozatali folyamatok automatizálására szolgáló technikai megoldásoktól,[501] továbbá az MI alkalmazása esetén is csak azon esetekben alkalmazhatók a GDPR automatizált döntéshozatallal, illetve profilalkotással kapcsolatos rendelkezései, amikor az MI által hozott döntés az alábbiak szerinti hatással jár, amely az emberi döntést segítő vagy támogató működésen túlmutató, kellően autonóm döntési folyamat eredménye.

[498] Open Future, Defining best practices for opting out of ML training, https://openfuture.eu/wp-content/uploads/2023/09/Best-_practices_for_optout_ML_training.pdf. 7-8.
[499] Garante, Avviso di indagine conoscitiva in materia di webscraping, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9972153
[500] GDPR 22. cikk
[501] CHRONOWSKI, KÁLMÁN, SZENTGÁLI-TÓTH i. m. 11.

Adott esetben azonban vita tárgyát képezheti, hogy az MI által meghozott döntés joghatással vagy ahhoz hasonló jelentős hatással jár-e az érintettre nézve. Joghatással járhat például egy szerződéskötés vagy szociális juttatás megtagadásával járó döntés, hasonló jelentős hatással pedig például egy, az érintett választási szabadságát érdemben befolyásoló, hosszútávú, vagy az érintett helyzetére jelentős hatással bíró döntés (például: hitelnyújtással, egészségügyi szolgáltatások igénybevételével kapcsolatos döntés).[502] Így amennyiben például egy bank kölcsönszerződés megkötésére, és az érintett hitelkockázatának ezt megelőző kiszámítására használ MI-rendszert, és az érintettel való szerződéskötést az MI döntésétől teszi függővé, ez esetben joghatással járó döntésről beszélhetünk, míg amennyiben egy szolgáltató MI-rendszer segítségével dönt bizonyos kedvezmények nyújtásáról, úgy jellemzően joghatáshoz hasonló jelentős hatásról beszélhetünk.

MI alkalmazása esetén azonban csak akkor alkalmazhatók a GDPR automatizált döntéshozatalra, illetve profilalkotásra vonatkozó rendelkezései, amennyiben a döntést ténylegesen az MI hozza meg, vagy a döntéshozatal során az MI dominál. Amennyiben ugyanis az MI kizárólag döntéstámogató, illetve segítő funkciót képvisel, és a döntést emberi ügyintéző, illetve szakértő hozza meg, úgy automatizált döntéshozatalról nem beszélhetünk. Így tehát, amennyiben a fenti példánál maradva a kölcsönszerződéshez kapcsolódó kockázati besorolásról és a kölcsönszerződés megkötéséről ténylegesen a bank emberi ügyintézői, illetve szakértői döntenek, és az adott MI alapú megoldás például csak kisebb jelentőségű számítási vagy adminisztratív feladatokat lát el, úgy automatizált döntéshozatalra ténylegesen nem kerül sor.[503] Az EUB gyakorlata értelmében azonban már nem feltétlenül ez a helyzet olyan esetekben, ahol például az MI-rendszert hitelbírálat végzésére használják. Az adott természetes személy jövőbeli fizetési kötelezettségeinek teljesítésével kapcsolatos képességre vonatkozó valószínűségi érték automatizált megállapítása ugyanis már automatizált egyedi döntésnek tekintendő.[504] Mivel a pontozásra, értékelésre épülő rendszerek az ezek által kifejtett hatásokat, emberi magatartás befolyásolását ragadják meg, illetve sok esetben teszik pénzzé, így e tekintetben az adatvédelmi jognak is arányos választ kell adnia a személyes adatok efféle

[502] Az Adatvédelmi Munkacsoport automatizált döntéshozatallal és profilalkotással kapcsolatos wp251.rev.01 sz 2017. október 3-án meghozott, 2018. február 6-án felülvizsgált iránymutatása („**Automatizált Döntéshozatallal és Profilalkotással kapcsolatos Iránymutatás**"), 21-22.
[503] Lásd: Automatizált Döntéshozatallal és Profilalkotással kapcsolatos Iránymutatás, 9.
[504] C-634/21. sz. ügy OQ és a Land Hassen között, a SCHUFA Holding AG részvételével folyamatban lévő eljárásban [ECLI:EU:C:2023:957] 73. pont

felhasználására.[505] Hangsúlyozandó azonban, hogy az automatizált döntéshozatal megléte, valamint annak érintettre gyakorolt hatásai jellemzően csak esetről-esetre ítélhetők meg, illetve mérhetők fel, így az adatkezelőnek még az adott megoldás alkalmazása előtt különös gonddal kell vizsgálnia a fenti szempontokat, a teljes döntési folyamat, valamint az alkalmazás gyakorlati jelentőségének figyelembevételével. A döntéshozatal „emberi" jellegének megőrzése kapcsán nem elegendő például, ha a döntés megalapozását ténylegesen az MI által szolgáltatott eredmények szolgáltatják, amelyek érdemi felülvizsgálata nélkül hoz egy emberi ügyintéző pusztán formális döntést, ilyen esetekben ugyanis automatizált döntéshozatalra kerül sor a formális emberi közreműködés ellenére is.[506]

Tekintettel arra, hogy az automatizált döntéshozatal, illetve a profilalkotás kiemelt hatásokkal bírhat az érintettek jogaira és szabadságaira nézve, így annak alkalmazását a GDPR kizárólag meghatározott esetekben, illetve jogalapokra hivatkozással teszi lehetővé, ideértve azon esetet, ha az automatizált döntéshozatal, illetve a profilalkotás alkalmazása

- az érintett és az adatkezelő közti szerződés megkötéséhez vagy a szerződés teljesítéséhez szükséges,
- az alkalmazását az adatkezelőre alkalmazandó uniós vagy tagállami jog lehetővé teszi, és e körben az érintett jogainak, szabadságainak, valamint jogszerű elvárásainak védelmét garantáló intézkedéseket határoz meg, illetve
- az érintett kifejezett hozzájárulásán alapul.[507]

Kiemelendő, hogy amennyiben az automatizált döntéshozatallal, illetve profilalkotással járó adatkezelés a fentebb írtak szerint az érintett kifejezett hozzájárulásán alapul vagy szerződéskötéshez, illetve szerződés teljesítéséhez szükséges, úgy az adatkezelőnek további intézkedéseket kell tennie az érintett jogainak védelme érdekében, ideértve legalább az érintett jogát emberi beavatkozás kérésére, álláspontja kifejtésére, valamint a fentiek szerint hozott döntéssel szembeni kifogás benyújtására.[508] Így tehát, amennyiben az érintett hozzájárulása alapján nyújt a részére az adatkezelő MI megoldás elemzésével ajánlatokat, úgy az érintett kérheti, hogy ezen ajánlatokat emberi ügyintéző is vizsgálja felül (például: számítási hiba okán vagy egyéb okból kedvezőtlenebb ajánlat nyújtása esetén), továbbá a döntés, és így jelen

[505] Nello CRISTIANINI, Teresa SCANTAMBURLO: On social machines for algorithmic regulation, *AI & Society*, 2020/35, https://doi.org/10.1007/s00146-019-00917-8. 651.
[506] Lásd: Automatizált Döntéshozatallal és Profilalkotással kapcsolatos Iránymutatás, 22.
[507] GDPR 22. cikk (2) bek.
[508] GDPR 22. cikk (3) bek.

esetben az ajánlat, valamint annak meghozatala, alapul fekvő és felhasznált információk kapcsán észrevételeket tehet, és kifogással élhet az adatkezelőnél az MI által hozott döntéssel szemben.

A GDPR a fentieken túl rendelkezik az azonosítást nem igénylő adatkezelésekről is, amelyek az MI általi adatkezelések esetén különösen relevánsak lehetnek. Így amennyiben az adatkezelés célja már nem teszi szükségessé az érintett azonosítását, ennek kapcsán az érintettet azonosító kiegészítő információkat az adatkezelő nem köteles megőrizni, beszerezni, vagy egyébként kezelni az érintett azonosítása, és így a GDPR-nak való megfelelés érdekében.[509] Ennek megfelelően, amennyiben egy szervezet például MI alapú adatkezelés során a továbbiakban anonimizált adatkezelést kíván folytatni, arra tekintettel, hogy az érintettek azonosítására már nincs szükség, úgy az érintettet nem köteles újból azonosítani, mivel az adatkezelés célja már nem igényli személyes adatok kezelését. Amennyiben azonban az adatkezelő bizonyítani tudja, hogy nem képes az érintett azonosítására, úgy lehetőség szerint köteles őt erről tájékoztatni. Ebben az esetben az érintett joggyakorlásával kapcsolatos rendelkezéseknek sem szükséges megfelelnie az adatkezelőnek, kivéve, ha az érintett kifejezetten az azonosítását lehetővé tevő kiegészítő információkat nyújt az adatkezelő részére.[510]

g. Az adatvédelmi és az alapjogi hatásvizsgálat

A GDPR alapvető követelményként határozza meg az ún. beépített, valamint az alapértelmezett adatvédelem elvét. Ennek értelmében az adatkezelő „*a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába*” (beépített adatvédelem).[511] Mindemellett az adatkezelő „*megfelelő*

[509] GDPR 11. cikk (1) bek.
[510] GDPR 11. cikk (2) bek.
[511] GDPR 25. cikk (1) bek.

technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek" (alapértelmezett adatvédelem).[512] A beépített adatvédelem követelménye kiterjed mind az adatok mennyiségére, mind az adatkezelés mértékére, továbbá az adatkezelés időtartamára és az adatokhoz való hozzáférés jogának gyakorlására is. A beépített adatvédelem elvére tekintettel alkalmazott intézkedéseknek továbbá biztosítaniuk kell, hogy alapértelmezés szerint a gyűjtött adatok ne válhassanak meghatározatlan számú személy (ideértve például: az érintett számára ismeretlen, nagy számú további szolgáltató) számára hozzáférhetővé.[513] A fentiekre tekintettel az MI-rendszerek szolgáltatóitól is elvárható, hogy lehetőség szerint már a rendszerek tervezése során olyan megoldásokat építsenek a rendszerbe, illetve olyan eljárásokat alakítsanak ki, amelyek garantálják az érintettek jogainak és szabadságainak védelmét.

A fenti elvekre, valamint az adatkezelés egyes kiemelten kockázatosnak tekinthető eseteire, a GDPR hatásvizsgálat elvégzését határozza meg. Így amennyiben „*az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*", úgy az adatkezelő köteles az adatkezelés megkezdését megelőzően adatvédelmi hatásvizsgálatot végezni, amelyben számot ad az adatkezelésnek az érintett adatvédelmi jogaira gyakorolt hatásairól.[514] Az adatvédelmi hatásvizsgálat részleteit, lefolytatásának lépéseit, valamint annak eredményét, következtetéseit a gyakorlatban jellemzően egy adatvédelmi hatásvizsgálati dokumentáció foglalja össze, amelynek segítségével az adatkezelő az adatkezelés jogszabályi és adatvédelmi hatósági gyakorlatnak való megfelelését is igazolni képes. Az adatvédelmi hatásvizsgálat keretében továbbá az adatkezelőnek az adatkezelési művelet körülményeinek és az érintett érdekeinek figyelembevételével olyan intézkedéseket szükséges végrehajtania, amely garantálja az érintett jogainak és érdekeinek védelmét; ezen intézkedéseket szükséges az adatvédelmi hatásvizsgálati dokumentációban is egyértelműen megjeleníteni. Így például, ha az adott MI-rendszert közlekedési területen való megfigyelésére, illetve közlekedési adatok elemzésére használják, úgy a közlekedési adatok kezelése kapcsán az adatkezelőnek ajánlott lehet adott esetben az érintett által látogatott területek és az érintett útvonalának sajátosságait is figyelembe venni,

[512] GDPR 25. cikk (2) bek.
[513] Uo.
[514] GDPR 17. cikk (3) bek.

adott esetben pedig az útvonal kezdetére és végére vonatkozó információkat törölni, annak érdekében, hogy az érintett az általa használt útvonal alapján ne legyen azonosítható.[515]

Az adatvédelmi hatásvizsgálat különös jelentőséggel bírhat az olyan esetekben, ahol bizonyos adatkészleteket az adott MI-rendszer fejlesztéséhez használnak. Így például, amennyiben egy biztosítótársaság MI-rendszert alkalmaz ügyfélprofilok létrehozására és biztosítási kockázat kiszámítására, ennek kapcsán pedig – megfelelő jogalap meglétét, illetve jogszerű adatkezelést feltételezve – a meglévő ügyfélbázisában szereplő adatokat használ fel a rendszer fejlesztéséhez, úgy e körben kiemelt fontossággal bírhat naprakész információk felhasználása (például: korábbi ügyfelekre vonatkozó, illetve megszűnt biztosítási szerződésekhez kapcsolódó információk kezelésének elkerülése), valamint a rendszer megfelelő tesztelése. Mindemellett a rendszer éles alkalmazását követően is fontos az eredmények felülvizsgálata és a rendszer szükség esetén való módosítása.[516]

Fontos megemlíteni, hogy az MI Rendelet nagy kockázatú MI-rendszereket alkalmazó, közszféra által szabályozott szervezetek vagy közszolgáltatást nyújtó magánszervezetek, továbbá hitelértékesítést végző, valamint élet- és egészségügyi biztosítás területén kockázatértékelés és árazás kapcsán alkalmazott nagy kockázatú MI-rendszerek alkalmazói esetén ún. alapjogi (illetve az újabb fordításában alapvető jogi) hatásvizsgálat elvégzését írja elő a rendszer alapjogokra gyakorolt hatásainak értékelésével kapcsolatosan.[517] A hatásvizsgálatnak szükséges tartalmaznia különösen a rendszer alkalmazójának azon eljárása leírását, amelyben a nagy kockázatú MI-rendszer felhasználásra kerül a rendeltetésével összhangban, továbbá a rendszer alkalmazásának tervezett időtartamát, rendszerességét, a természetes személyek kategóriáit, csoportjait, akiket valószínűleg a rendszer alkalmazása érint, valamint az ezeket valószínűleg érintő hátrányok kockázatait, az emberi felülvizsgálattal kapcsolatos intézkedések leírását, továbbá a kockázatok materializálódása esetén alkalmazandó intézkedéseket.[518]

Megjegyzendő, hogy az alapjogi hatások mérése kapcsán eddig kevés iránymutatás született. A szakirodalomból érdekes példának tekinthető az Intesa Sanpaolo bankcsoport munkatársai által

[515] EDPB 4/2019. számú iránymutatás („**4/2019. sz. Iránymutatás**") a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat, elfogadás időpontja: 2020. október 20. 24.
[516] 4/2019. sz. Iránymutatás, 26.
[517] MI Rendelet 27. cikk (1) bek
[518] Uo.

kidolgozott „*Fundamental Rights and Artificial Intelligence Impact Assessment*”, röviden: „**FRAIIA**” elnevezésű hatásvizsgálat, illetve módszertan, amely egy kérdőívből, valamint egy kvantitatív mátrixból áll, részleteiben elemezve az adott rendszer alapjogokra gyakorolt hatásait, továbbá magában foglalva egy analitikai eszközt is.[519] A fenti hatásvizsgálat elenyészőtől nagyon magasig (0-4) kategorizálja az alapjogi kockázatokat. A közepest el nem érő kockázatok (0-1) esetén az MI-rendszer megfelelőnek tekinthető, míg a közepes (2) és a magas (3) kockázat között a kockázatok csökkentésére, és/vagy a megfelelő figyelemmel kísérésére további intézkedések ajánlottak, míg a magas kockázatot elérő vagy meghaladó rendszerek nem fejleszthetők tovább.[520] Emellett szintén iránymutatást nyújthat a holland kormány által a közszféra számára készített alapjogi és algoritmusokkal kapcsolatos hatásvizsgálati dokumentuma („*Impact Assessment Fundamental Rights and Algorithms*”).[521] A dokumentum többféle szempontot is kiemel, amelyet adott esetben a magas kockázatú MI-rendszerek alkalmazóinak tanácsos lehet megjeleníteniük az alapjogi hatásvizsgálatban, ideértve például olyan közös értékeket, amiknek az elérésére az adott algoritmus törekszik,[522] illetve érdekmérlegelési teszt elvégzését, különösen alapjogok ütközése esetén.[523] Emellett a dokumentum javasolja az állampolgárok bevonását a hatásvizsgálati folyamatba, ideértve például az algoritmus esetleges pozitív, illetve negatív hatásaival kapcsolatos kérdések megvitatását.[524] A dokumentum továbbá szintén javasolja kilépési stratégia elkészítését, ha az algoritmus a továbbiakban már nem kerülne fejlesztésre.[525]

Hangsúlyozandó, hogy az MI Rendelet értelmében a hatásvizsgálat elkészítésének kötelezettsége a rendszer első alkalmazására vonatkozik, az alkalmazók pedig a későbbi alkalmazások esetén támaszkodhatnak a korábban, például a szolgáltató által készített alapjogi hatásvizsgálatra.[526] A hatásvizsgálat elvégzéséről azonban az alkalmazónak a piacfelügyeleti hatóságot is értesítenie kell.[527] Habár ezt az MI Rendelet nem részletezi, logikusnak tűnhet,

[519] Samuele BERTAINA, Ilaria BIGANZOLI, Rachele DESIANTE, Dario FONTANELLA, Nicole INVERARDI, Ilaria Giuseppina PENCO, Andrea COSENTINI: Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act. https://ssrn.com/abstract=4698609, http://dx.doi.org/10.2139/ssrn.4698609. 9.
[520] Ibid. 25-26.
[521] Government of the Netherlands, Impact Assessment Fundamental Rights and Algorithms, 2022.03.31, https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms
[522] Ibid. 14.
[523] Ibid. 15.
[524] Ibid. 15.
[525] Ibid. 21.
[526] MI Rendelet 27. cikk (2) bek.
[527] MI Rendelet 27. cikk (3) bek.

hogy amennyiben a rendszer jelentősen módosításra kerülne, vagy a rendeltetésének célja megváltozna, úgy az alkalmazóktól szükség szerint elvárható, hogy felülvizsgálják a hatásvizsgálati dokumentációt vagy új hatásvizsgálatot végezzenek. Ilyen esetekben akár a piacfelügyeleti hatóság újbóli értesítése is szükségessé válhat a megváltozott körülményekről, illetve az alapjogi hatásvizsgálat felülvizsgálatáról, újbóli elvégzéséről.

Az MI Rendelet az alapjogi hatásvizsgálat kapcsán leszögezi továbbá, miszerint az alapjogi hatásvizsgálat az adatvédelmi hatásvizsgálattal együttesen is elvégezhető,[528] illetve a két vizsgálat – a megfelelő áttekinthetőség biztosítása mellett – akár közös dokumentációba is foglalható. Mindez azért is fontos, mivel az adatvédelmi hatásvizsgálatot a természetes személyek jogaira és szabadságaira jelentett magas kockázatú adatkezelések esetén kötelesek elvégezni az adatkezelők, ez pedig adott esetben kiterjedhet az adatvédelmi jogokon túli egyéb alapvető jogokra is.[529] Így ha ilyen értékelést az adatvédelmi hatásvizsgálat már tartalmaz, azt az alapjogi hatásvizsgálatnak nem feltétlenül kell újra megjelenítenie (elegendő lehet például e körben az adatvédelmi hatásvizsgálatra hivatkozás, illetve arra támaszkodás). Emellett az MI Rendelet értelmében az MI-hivatal is kérdőívmintát fog kidolgozni az alapjogi hatásvizsgálattal kapcsolatos kötelezettségeknek történő egyszerűsített módon való megfelelést.[530]

Megemlítendő továbbá, hogy bár az alapjogi hatásvizsgálat elvégzése fontos szempontot képezhet a fentiek szerinti MI-rendszerek alkalmazása során, a gyakorlatban így is számos kérdés felmerül, például az érintett alapjogok és az adott rendszer arra gyakorolt hatásainak felmérésével kapcsolatban (ideértve például egy közszolgáltató egészségügyi szolgáltatásai során vagy egy bank hitelértékeléshez használt MI-rendszerének alapjogi hatásai felmérése kapcsán, amelyek a gyakorlatban igen nehezen beláthatók lehetnek).[531] A fentiek okán valószínűleg kiemelt jelentőséggel fog bírni az egyes szakterületeken eljáró hatóságok iránymutatása az adott típusú MI-rendszerekre vonatkozó alapjogi hatásvizsgálatok elkészítése tekintetében.

h. A mesterséges intelligencia és az adatvédelmi tisztviselő

[528] MI Rendelet 27. cikk (4) bek.
[529] Heleen JANSSEN, Michelle SENG AH LEE, Jatinder SINGH: Practical fundamental rights impact assessments, *International Journal of Law and Information Technology*, vol. 30, issue 2. (Summer 2022), https://doi.org/10.1093/ijlit/eaac018. 210.
[530] MI Rendelet 27. cikk (5) bek.
[531] ZŐDI Zsolt: Fából vaskarika? Alapjogi hatásvizsgálat a Mesterséges Intelligencia Rendeletben, 2024.03.08, https://www.ludovika.hu/blogok/itkiblog/2024/03/08/fabol-vaskarika/

Az adatvédelmi tisztviselő az adatkezelő, illetve adatfeldolgozó által kijelölt, adatvédelmi ügyekben jártas olyan személy, aki, illetve amely az adatkezelőt, illetve adatfeldolgozót adatvédelmi ügyekben támogatja, az adatvédelmi jogszabályi megfelelést biztosítja, szakmai tanácsot ad az adatkezelő, illetve adatfeldolgozó részére (ideértve például: adatvédelmi hatásvizsgálat elvégzése kapcsán), továbbá együttműködik a felügyeleti hatósággal, illetve kapcsolattartó pontként szolgál.[532]

Az adatvédelmi tisztviselőnek jogi vagy egyéb (például: informatikai) szakképzettséggel nem szükséges rendelkeznie, azonban szakmailag rátermettnek kell lennie, és megfelelő, gyakorlati szintű ismerettel kell bírnia adatvédelmi kérdésekben.[533] Habár az adatvédelmi tisztviselő rátermettsége jellemzően nehezen mérhető, illetve ennek kapcsán nehezebben határozhatók meg kritériumok,[534] nagyobb szervezeteknél gyakorinak tekinthető, hogy jogi, illetve – különösen technológiai nagyvállalatok esetén – informatikai szakember kerül kijelölésre adatvédelmi tisztviselőként, még kisebb szervezetek (ideértve például: kis- és középvállalkozások) esetén jellemzőnek mondható egy-egy adatvédelmi ügyek kezelésére kijelölt, adatvédelmi tréningen részt vett munkatárs vagy külső szakértő (például: megbízási szerződés alapján eljáró ügyvéd) kijelölése. Különösen szervezeten belüli pozíciók esetén azonban kiemelten fontosnak tekinthető olyan személy kiválasztása, akinek az esetleges további feladatai és kötelezettségei nem ütköznek az adatvédelmi tisztviselői pozícióból fakadó feladatokkal, kötelezettségekkel.[535] Így például összeférhetetlenséghez vezethet szervezeten belüli egyéb vezető pozíció (például: vezérigazgató, HR igazgató) betöltése, rövid vagy határozott idejű munkaviszony, alacsonyabb szintű vezetőknek történő közvetlen jelentési kötelezettség.[536] Ennek kapcsán megjegyzendő, hogy akár külső tanácsadók esetén is felmerülhet összeférhetetlenség (ha például az adatvédelmi tisztviselőként megbízott ügyvédnek a bíróság előtt kell az adatkezelő álláspontját képviselnie); így tekintettel arra, hogy a gyakorlatban számtalan összeférhetetlenségi kérdés felmerülhet, ezért ajánlott lehet az összeférhetetlenséggel kapcsolatos szabályokat belső szabályzatban is rögzíteni.[537]

[532] GDPR 38. cikk (1) bek., 39. cikk (1) bek.
[533] 37. cikk (5) bek.
[534] Francesco CICLOSI, Fabio MASSACCI: "The Data Protection Officer: A Ubiquitous Role That No One Really Knows". *IEEE Security & Privacy*, vol. 21, no. 01. (2023). doi: 10.1109/MSEC.2022.3222115. 75.
[535] GDPR 38. cikk (6) bek.
[536] EDPS, Data Protection Officer (DPO), https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
[537] SZABÓ Endre: Az adatvédelmi tisztviselőről. A GDPR szabályainak elemzése. *Infokommunikáció és jog*, 2018/1. 7.

Adatvédelmi tisztviselővé kijelölhető továbbá akár jogi személy (például: gazdasági társaság) is, ilyen esetekben azonban elvárható olyan természetes személy további kijelölése, tulajdonképpeni delegálása a jogi személy részéről, aki az adatvédelmi tisztviselői tevékenységet ténylegesen ellátja, és személyében is megfelel az adatvédelmi tisztviselővel szemben támasztható szakmai tudással kapcsolatos elvárásoknak. Így például egy MI-rendszereket fejlesztő vállalkozás esetén elengedhetetlennek tűnik, hogy az adatvédelmi tisztviselő ismerje az MI-rendszerekkel kapcsolatos szabályozást, valamint megfelelő ismeretei legyenek az MI-rendszerek működéséről, az ezzel kapcsolatos adatvédelmi szempontokról.

A GDPR meghatározza azon eseteket, amikor adatvédelmi tisztviselő kijelölése kötelező, ideértve

- a közérdekű szervek vagy közhatalmi feladatokat ellátó szervek általi adatkezelést (ide nem értve az igazságszolgáltatási feladatkörükben eljáró bíróságokat),
- az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését szükségessé tevő fő tevékenységet folytató adatkezelőket, illetve adatfeldolgozókat,
- különleges adatokat, illetve büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatokat fő tevékenységként nagy számban kezelő adatkezelőket, illetve adatfeldolgozókat.[538]

Természetesen adatvédelmi tisztviselő olyan esetekben is kijelölhető, ha arra az adatkezelő a fentiek szerint nem lenne köteles. Vállalkozáscsoport[539] emellett közös adatvédelmi tisztviselőt is kijelölhet, ha ez valamennyi tevékenységi helyről könnyen elérhető,[540] így például valamennyi olyan országban, illetve területen képes az adatkezelési folyamatokat felügyelni, illetve a hatósággal és érintettekkel való kommunikációba bekapcsolódni, ahol a vállalkozáscsoport tagjai jelen vannak. Erre adott esetben sor kerülhet akár MI-rendszer támogatásával is, amely például segítséget nyújt az érintetti kérelmek vagy hatósági megkeresések lefordításában, kezelésében.

[538] GDPR 37. cikk (1) bek.
[539] GDPR 4. cikk 19. pontja szerint vállalkozáscsoportnak minősül „*az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások.*”
[540] GDPR 37. cikk (2) bek.

Természetesen az adatvédelmi tisztviselő működéséhez, valamint tevékenységének sikeres ellátásához az adatkezelő, illetve az adatfeldolgozó köteles megfelelő forrásokat biztosítani.[541] Ezen források körébe tartozhatnak MI alapú vagy egyéb magas szintű technológiai megoldások is, figyelembe véve az adatkezelő, illetve adatfeldolgozó, valamint az általa folytatott tevékenységek, adatkezelési műveletek sajátosságait. Például nagy mennyiségű személyes adatot tartalmazó adatbázisokat, illetve ezekkel kapcsolatos MI-rendszert üzemeltető adatkezelőnek szükséges lehet olyan informatikai megoldások alkalmazásáról gondoskodnia, amelyek lehetővé teszik az egyes érintettekre vonatkozó információk hatékony keresését, kiválasztását, adott esetben a vonatkozó adatbázisból való eltávolítását. Ilyen esetben az adatvédelmi tisztviselőnek vagy az adatkezelő által e célra kijelölt más segítő személynek is szükséges lehet az adatvédelmi megfelelés biztosítása, illetve a kapcsolódó érintetti megkeresések hatékony teljesítése érdekében a fenti rendszer működésével kapcsolatos megfelelő ismereteket birtokolnia. Ennek kapcsán az adatkezelőnek adott esetben az adatvédelmi tisztviselő, illetve más segítő személy informatikai képzését is szükséges biztosítania.

A fentieken túl kiemelendő továbbá az adatvédelmi tisztviselő függetlenségének fontossága, tekintettel arra, hogy az adatvédelmi tisztviselő feladatai ellátásával kapcsolatban utasításokat nem fogadhat el, illetve azzal összefüggésben nem bocsátható el, vagy nem szankcionálható, és kizárólag az adatkezelő, illetve adatfeldolgozó legfelső vezetésének tartozik felelősséggel.[542] Erre tekintettel például az adatvédelmi tisztviselőt az adatkezelő társaság egyes szakterületeinek vezetői nem utasíthatják meghatározott dokumentumok vagy folyamatok jóváhagyására, illetve ennek hiánya esetén nem is szankcionálhatják.

Az adatvédelmi tisztviselő kijelölése, valamint tevékenységének végzése kapcsán felmerülhet a kérdés, hogy ezen feladatokra feltétlenül szükséges-e „emberi” szakértő kijelölése, és nem elegendő-e például egy MI alapú megoldás alkalmazása? Ennek kapcsán vitán felül áll, hogy az adatvédelmi tisztviselő tevékenységét a gyakorlatban technikai megoldások, szoftveres alkalmazások is segíthetik (például: analitikai eszközök),[543] azonban egy kellően fejlett MI megoldás akár képes lehet arra is, hogy az adatvédelmi tisztviselő feladatait is ellássa, és ne csak támogassa azokat. Ha napjainkban még nem is, a közeljövőben azonban elképzelhető

[541] GDPR 38. cikk (2) bek.
[542] GDPR 38. cikk (3) bek.
[543] CICLOSI, MASSACCI op. cit. 76.

olyan MI-rendszer kifejlesztése, amely már képes lehet egy adott szervezet, illetve vállalkozáscsoport adatvédelmi tisztviselői feladatait ellátni, akár egy emberi szakértőnél hatékonyabban is (például: beépített fordítási megoldásokkal, az EU-n vagy egyéb térségen belül valamennyi tagállam releváns jogszabályainak és adatvédelmi hatósági, valamint bírósági gyakorlatának figyelemmel kísérésével). Ilyen esetekben azonban vélhetőleg pont az emberi ítélőképesség, valamint a szakmai és jogi értelemben vett felelősség hiánya okán kérdőjelezhető meg az MI adatvédelmi tisztviselői pozíció betöltésére való alkalmassága. Hiszen még a jogi személyek jogi, illetve – vezetőiken, munkavállalóikon keresztül – közvetve szakmai értelemben is elszámoltathatók, úgy egy MI-rendszer önmagában nem vonható felelősségre, és nem várható el tőle az emberihez vagy akár egy jogi személyhez hasonló tevékenységszervezés sem.

A fentiekre tekintettel megállapítható, hogy amennyiben MI alapú megoldás kerül alkalmazásra adatvédelmi tisztviselői feladatok ellátása során, úgy nem maradhat el az ezen megoldást felügyelő emberi szakértő kijelölése sem. Ha pedig jogi személy kínál ilyen MI alapú megoldást, úgy ugyancsak szükséges olyan emberi szakértőt kijelölnie, amely képes ezen megoldás tevékenységének, illetve az általa hozott döntések áttekintésére és jóváhagyására, szükség szerinti felülvizsgálatára, valamint erre tekintettel felelősség vállalására. Természetesen azonban a fentebb írt „MI adatvédelmi tisztviselőknél” valószínűbbnek tűnhet az adatvédelmi tisztviselőket, valamint a vállalkozások adatvédelmi megfelelését segítő MI alapú megoldások elterjedése, tekintettel arra, hogy ilyen megoldásokat számos vállalkozás, illetve egyéb szervezet már napjainkban is alkalmaz.

i. A mesterséges intelligencia és az adatbiztonság

Az adatbiztonság megfelelő szintje, valamint a megfelelő adatbiztonsági intézkedések alkalmazása az MI kapcsán is kiemelt jelentőséggel bír. Ezt különösen indokolják az automatizált döntéshozatallal, valamint a magas szintű MI-rendszerek alkalmazásával kapcsolatos kockázatok, illetve az MI általi adatkezelés megfelelősége is.

A GDPR az adatbiztonsággal kapcsolatos definíciót nem tartalmaz, azonban általánosságban előírja, hogy „*az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és*

súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja".[544] E körben továbbá a GDPR példákat is meghatároz (ideértve például a személyes adatok titkosítását vagy álnevesítését).[545] A fentiek körében kiolvasható továbbá, hogy az adatbiztonság körében a GDPR megfelelő technikai és szervezési intézkedések alkalmazását követeli meg, így az adatkezelő vagy adatfeldolgozó által alkalmazott adatbiztonsági intézkedések körét alapvetően két csoportra bontja.

A technikai intézkedések körébe tartoznak például a megfelelő védelmi szoftverek, továbbá a rendszerek fizikai védelme, míg a szervezési intézkedések körbe tartoznak az adatkezelő szervezési intézkedései révén elért adatbiztonsági megoldások, eljárások és szabályozás, ideértve például az adatkezelő munkatársaira vagy egyes adatkezelésekre irányadó, illetve átfogó adatvédelmi és adatbiztonsági szabályzatot,[546] a személyzet részére nyújtott adatbiztonsági képzést, tréninget. Az adatbiztonság területén gyakran alkalmazott szabályzatok közé tartoznak továbbá a különböző technológiák alkalmazásával kapcsolatos szabályzatok, például kamerarendszer alkalmazásával kapcsolatos szabályzat,[547] információbiztonsági, illetve iratkezelési szabályzatok, valamint az adatvédelmi incidensek kezelésével kapcsolatos szabályzat.[548]

Az MI fejlesztése és alkalmazása esetén is számos olyan technikai, illetve szervezési intézkedésről beszélhetünk, amelyek hatékonyan lehetnek képesek védeni az MI által kezelt személyes adatokat. E körbe tartozhat például álnevesített, anonimizált, illetve szintetikus adatok felhasználása, amely így az érintettek számára nagyobb fokú védelmet nyújthat, illetve ez által – különösen az anonimizált, illetve a konkrét személyekhez nem kapcsolható szinsztetikus adatok kezelése révén – elkerülhető a személyes adatok kezelése, és így az adatvédelmi szabályoknak történő megfelelés. Ezen esetekben azonban az adatkezelőnek különös figyelmet kell fordítania az érintett azonosíthatóságának lehetőségére. Összhangban a

[544] GDPR 32. cikk (1) bek.
[545] Uo.
[546] BALOGH Zsolt György, KISS Attila, POLYÁK Gábor, SZÁDECZKY Tamás, SZŐKE Gergely László: Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén. *Pro Futuro*, 2014/1. https://doi.org/10.26521/Profuturo/2014/1/5494. 41.
[547] Lásd például az ír adatvédelmi hatóság gyakorlatából: DPC, Guidance on the Use of CCTV – For Data Controllers, version last updated: May 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controllers_0.pdf. 4.
[548] DPC, Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR, October 2019, http://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide. 18.

személyes adat fogalma kapcsán előadottakkal ugyanis az érintett azonosíthatóságának a technológiai fejlődésre, valamint az MI alkalmazására tekintettel jelentős kockázata lehet olyan esetekben is, ahol az adat és az érintett közti kapcsolat látszólag már megszűnt vagy az adott időpontban, illetve körülmények között már nem áll fenn. Ez azért is fontos, mert sokáig az anonimizálást egyfajta „aduásznak" tekintették az adatvédelem területén, bízva abban, hogy az érintettet azonosító egy-egy információ eltávolításával – és így az adat és az érintett közti kapcsolat megszüntetésével – egyben a személyes adatok védelmét is egy magasabb szintre helyezhetik.[549] Mindezen bizakodást azonban a technológiai fejlődés, és az MI fejlődése napjainkra már meggyengítette, növelve az érintettek újra azonosíthatóságával kapcsolatos kétségeket.

Hasonló kétségek merülhetnek fel továbbá az álnevesített adatkészletek kapcsán is, az ezzel kapcsolatos védelmi intézkedések ugyanis sokszor kijátszhatók, egyben az adatok további felhasználhatóságát is jellemzően megnehezítik, gátat szabva az MI általi felhasználásnak, valamint a vonatkozó információk megfelelő kiaknázásának. Az érintett közvetlen, vagy például egyes szokásain, viselkedésén alapuló, közvetett újbóli azonosíthatóságával kapcsolatos félelmek különösen az érintett azonosítását megszüntető intézkedéseken, az álnevesítés „visszafordításán" vagy különböző adatkészletek összevetésén alapulnak,[550] azonban pusztán a védelmi intézkedések meghaladottsága is vezethet az érintett újbóli azonosíthatóságához, valamint a személyes adatokkal kapcsolatos esetleges visszaélésekhez. A személyes adatok megfelelő védelme vonatkozásában így tökéletes megoldásról nem beszélhetünk, inkább a védelmi intézkedések jól összeállított kombinációja az, amivel a személyes adatok védelme az MI korában kellő mértékben garantálható lehet. Megemlítendő továbbá, hogy az anonimizáció vagy az álnevesítés a fentiektől függetlenül továbbra is hatékony megoldás lehet különösen zárt, a nyilvánosság számára nem elérhető adatkészletek esetén. Így a magyar alkotmánybírósági gyakorlat szerint megfelelőnek tekinthető például az anonimizálás levéltári anyag esetén, amennyiben az anonimizált iratanyagból az érintettre vonatkozóan nem lehet következtetést levonni, és így az érintettet azonosítani.[551] A fentiek alapján azonban az érintett azonosíthatósága könnyebben akadályozható meg hasonló papíralapú, illetve zárt adatkészletben lévő információk esetén, mint például az interneten

[549] Paul OHM: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, vol. 57. (2010), https://ssrn.com/abstract=1450006. 1706.
[550] Boris LUBARSKY: Re-Identification of „Anonymized" Data. *Georgetown Law Technology Review*, 1. (2017) 208–209.
[551] 3441/2020. (XII. 9.) AB végzés, [10]-[11].

keresztül hozzáférhető, illetve egyéb nagyobb, könnyen elérhető adatkészletben tárolt információk esetén.

Természetesen napjainkban már MI-specifikus, illetve az MI általi adatkezelés kapcsán különösen hatékonyan alkalmazható adatbiztonsági intézkedésekről is beszélhetünk, amelyek révén az adatkezelők adott esetben hatékonyabb módon lehetnek képesek megelőzni, illetve kezelni az MI általi adatkezeléssel kapcsolatos kockázatokat. E körben többféle adatvédelmet erősítő technika (angolul: „*privacy enhancing technologies*") is meghatározható, amelyek a kezelt adatok körének minimalizálása mellett az adatbiztonság szintjét is jelentősen megemelhetik, illetve az érintettek jogainak érvényesítését is biztosítják.[552] E körbe tartozik például a federatív tanulás (angolul: „*federated learning*"), amely lehetővé teszi az MI-modellek fejlesztése során a tanítóadatok külön kezelését, így a modellek fejlesztését végző személyek vagy szervezetek anélkül is egyesíthetik tanuláshoz használt modelljeiket, hogy a fejlesztéshez szükséges egyéb adatokat megosztanák.[553] Szintén hatékony adatbiztonsági megközelítést jelenthet például a homomorfikus titkosítás (angolul: „*homomorphic encryption*"), amely révén számítások végezhetők titkosított adatokon a titkosítás feloldása nélkül is,[554] valamint az ún. differenciált adatvédelem (angolul: „*differential privacy*"), amelynek révén egy adatbázis akként alakítható ki, hogy az abból nyerhető információk révén az érintett ne legyen azonosítható.[555]

Hangsúlyozandó azonban a fentebb írtakkal összhangban, hogy ezen technikák, illetve megoldások jellemzően nem biztosítanak önmagukban teljeskörű védelmét, szükséges azokat egyéb intézkedésekkel is kiegészíteni, illetve azokkal összhangban alkalmazni, ennek hiányában ugyanis az alkalmazott intézkedések elégtelennek, illetve kijátszhatónak bizonyulhatnak. Így például federatív tanulás alkalmazása esetén, az egyes modellek megvizsgálása, visszafejtése révén – közvetett módon – azonosíthatók az érintettek, illetve adataik, így jellemzően szükséges a federatív tanulást egyéb adatvédelmet erősítő technikákkal is kiegészíteni, mint például homomorfikus titkosítással vagy például biztonságos

[552] ICO, Chapter 5: Privacy-enhancing technologies (PETs). Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. September 2022, https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf ("**ICO PETs Iránymutatás**") 3.
[553] ICO PETs Iránymutatás, 23.
[554] ICO PETs Iránymutatás, 12.
[555] Cynthia DWORK: Differential Privacy. Velence (2006. július 10-14.): *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)* | July 2006, Sprinter Verlag, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf. 1, 9–11.

kommunikációs protokollok (angolul: „*secure communications protocols*") segítségével.[556] Erre tekintettel tehát az MI megoldást alkalmazó szervezeteknek az adatkezelés sajátosságait figyelembevéve szükséges meghatározniuk a szükséges körű védelmi intézkedéseket, és azokat az adatbiztonság megfelelő védelmi szintje által indokolt módon kell alkalmazniuk. Így például akár alacsonyabb szintű adatbiztonsági intézkedések alkalmazása is elegendő lehet egy jellemzően nem személyes adatok kezelésére szolgáló MI-rendszer fejlesztése esetén, míg például nagy számú egészségügyi és egyéb szenzitívnek mondható adatok kezelésére alkalmazott MI-rendszer kapcsán jellemzően számos adatbiztonsági intézkedés jól összehangolt alkalmazása szükséges. Hangsúlyozandó azonban, hogy az adatbiztonsági szempontokon túl az egyes MI-rendszerek kapcsán egyéb szempontok is irányadók lehetnek (például: szellemi tulajdon, üzleti titok védelme), továbbá az adott terület, tevékenység kapcsán irányadó specifikus jogszabályi követelmények, hatósági vagy szakmai gyakorlat is adott esetben figyelembe veendő az adatkezelők által (például: kockázatkezelési célú MI-rendszert alkalmazó biztosítótársaság általi adatkezelés esetén az MI Rendelet nagy kockázatú MI-rendszerekre irányadó szabályai, az irányadó adatvédelmi és egyéb jogszabályi rendelkezések, felügyeleti hatóság előírásai, iránymutatásai).

Az MI-modellek kapcsán további védelmet nyújthat az egyes, például jogsértő adatkezeléshez használt modellek megsemmisítése (angolul: „*model destruction*"), illetve a tanuláshoz használható adatok eltávolítása (*model disgorgement*),[557] valamint az egyes adatok „elfelejtése" (*model unlearning*). A törlés azonban értelemszerűen csak szűkebb esetben alkalmazható a problémás adatok és általuk érintett modellek megsemmisítésére, amennyiben például az adott modell alkalmazása meghaladja az észszerűen elvárható kockázatok körét.[558] A fentiekre tekintettel azonban akár egyes algoritmusok is megtaníthatók arra, hogy egyes személyes jellemzőket azonosítsanak és töröljenek, az adatok hatékony azonosítása és törlése azonban – különösen nagy nyelvi modellek alkalmazása esetén – a felhasználás kontextusának tükrében akadályokba ütközhet,[559] így az adatkezelőnek gondosan szükséges áttekintenie, mely

[556] ICO PETs Iránymutatás, 25-26.
[557] Brandon LALONDE: Explaining model disgorgement. *IAPP*, 2023.12.13, https://iapp.org/news/a/explaining-model-disgorgement/
[558] HUTSON, WINTERS op. cit. 134.
[559] Hannah BROWN, Katherine LEE, Fatemehsadat MIRESHGHALLAH, Reza SHOKRI, Florian TRAMÈR: What Does it Mean for a Language Model to Preserve Privacy?. Szöul (2022. június 21-24.): *ACM Conference on Fairness, Accountability, and Transparency (FAccT '22). ACM*, New York, USA, June 2022, https://doi.org/10.1145/3531146.3534642. 2287.

intézkedések lehetnek a leginkább alkalmasak az adott modell, illetve arra épülő rendszer sajátosságait is figyelembe véve a személyes adatok hatékony védelmére.

Az MI-rendszerek fejlesztése, adott rendszerkörnyezetbe való implementálása, illetve alkalmazása kapcsán ugyancsak kiemelt jelentőséggel bír az ún. *red teaming*, amely során az adott szervezet vagy megoldás védelmi képességei kerülnek felmérésre, illetve tesztelésre,[560] illetve a védelmi oldalra fókuszáló *blue teaming*, vagy az azok együttműködésére összepontosító *purple teaming*.[561] Mindezt kiegészíthetik ún. *adversarial machine learning*, röviden: „*AML*" eljárások, stratégiák is, amelyek során az adott gépi tanulással ellátott rendszert vizsgálják, illetve megkísérlik manipulálni a rendszer által adott eredmények, információk felhasználásával.[562] Hangsúlyozandó azonban, hogy egy személyes adatok kezelésére szolgáló rendszer elavultsága, illetve annak várható lecserélése nem mentesíti az adatkezelőt a megfelelő adatbiztonsági intézkedések alkalmazása alól, így ez esetben is szükséges az adatkezelőnek ilyen intézkedéseket alkalmaznia, amely a személyes adatok védelmére jelentett kockázatokkal arányos.[563] Ilyen lehet például az elavultnak tekinthető rendszerek fejlesztése, vagy új, megfelelő védelmi szintet biztosító megoldások bevezetése.

A fentiek mellett a nagy kockázatú MI-rendszerek esetén szükséges kockázatkezelési rendszer létrehozása, bevezetése, dokumentálása és fenntartása.[564] Az MI Rendelet értelmében a kockázatkezelési rendszer egy olyan megszakítás nélkül végzett iteratív folyamat, amelyet a nagy kockázatú MI-rendszer egész életciklusára terveztek, és amely azt végigkíséri, és amelyhez az adatok rendszeres és szisztematikus felülvizsgálatára és aktualizálására van szükség.[565] Ezen folyamat továbbá legalább a következő lépéseket tartalmazza:

- azon ismert, valamint észszerűen előre látható kockázatok azonosítása és elemzése, amelyek a nagy kockázatú MI-rendszer rendeltetésszerű használata esetén az egészségre, a biztonságra és az alapvető jogokra jelenthetnek,
- a nagy kockázatú MI-rendszer rendeltetésszerű használata, valamint észszerűen előre látható rendellenes használata esetén felmerülő kockázatok becslése és értékelése,

[560] IBM, Red teaming 101: What is red teaming?, https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/
[561] PlexTrac, What Is Purple Teaming?, https://plextrac.com/what-is-purple-teaming/
[562] National Cybersecurity Center of Excellence, Artificial Intelligence: Adversarial Machine Learning, https://www.nccoe.nist.gov/ai/adversarial-machine-learning
[563] ICO, Penalty Notice, COM0804337, Marriott International Inc., 30 October 2020. 6.59.
[564] MI Rendelet 9. cikk (1) bek.
[565] MI Rendelet 9. cikk (2) bek.

- egyéb esetlegesen felmerülő kockázatok értékelése a forgalomba hozatal utáni nyomonkövetési rendszerből gyűjtött adatok elemzése alapján,
- megfelelő és célzott kockázatkezelési intézkedések elfogadása az azonosított kockázatok kezelése érdekében.[566]

Emellett az MI Rendelet a modellek adatokkal való tanítását magukban foglaló technikákat használó nagy kockázatú MI-rendszerek kapcsán minőségi kritériumokat határoz meg, így ezen rendszereket ezen kritériumoknak megfelelő tanító-, validálási- és tesztadatkészletek alapján szükséges fejleszteni,[567] amelyeket megfelelő adatkormányzási és adatgazdálkodási gyakorlatoknak kell alávetni.[568] Ezen adatkészletek relevánsak, kellően reprezentatívnak, valamint – a rendeltetés szempontjából – a lehető legnagyobb mértékben hibáktól mentesek és teljesek kell, hogy legyenek. Emellett továbbá olyan statisztikai tulajdonságokkal kell rendelkezniük, amely megfelel azon érintetteknek vagy érintettek csoportjainak, akikkel vagy amelyekkel kapcsolatosan az adott rendszert használni kívánják. Ennek kapcsán kiemelendő, hogy az adatkészletek fenti jellemzői teljesíthetők az egyes adatkészleteknek vagy azok kombinációjának a szintjén.[569] A fentieken túl az adatkészleteknek továbbá a rendszer használata által indokolt egyéb releváns jellemzőket vagy elemeket is szükséges figyelembe venniük, ideértve azokat, amelyek az MI-rendszer alkalmazásának sajátos földrajzi, kontextuális, magatartási vagy funkcionális környezetéhez kapcsolódnak.[570] Megjegyzendő, hogy habár ezen további szempontok segítséget jelenthetnek tanító-, a validálási és a tesztadatkészletek megfelelő kiválasztása és alkalmazása kapcsán, e körben további, részletes adatminőségi követelményeket az MI Rendelet nem rögzít,[571] így kérdéses, ezen általános szempontok hogyan kerülnek majd figyelembevételre a gyakorlatban.

A nagy kockázatú MI-rendszerekhez kapcsolódóan továbbá a forgalomba hozatal, illetve üzembe helyezés előtt műszaki dokumentációt kell készíteni, valamint ezen dokumentációt naprakészen tartani, amely ellenőrizhető módon, világos és érthető formában bizonyítja a rendszer megfelelését az irányadó jogszabályi követelményeknek.[572] Ezen műszaki dokumentáció adott esetben része lehet egy nagyobb dokumentációnak vagy szabályzat-

[566] Uo.
[567] MI Rendelet 10. cikk (1) bek.
[568] MI Rendelet 10. cikk (2) bek.
[569] MI Rendelet 10. cikk (3) bek.
[570] MI Rendelet 10. cikk (4) bek.
[571] MEZEI i. m. 65.
[572] MI Rendelet 11. cikk (1) bek.

csoportnak is, azonban formájától, valamint más szabályzatoktól való kapcsolatától függetlenül is egyértelmű áttekintést kell nyújtania a nagy kockázatú MI-rendszer megfelelőségéről. Mind a műszaki dokumentáció elkészítése, mind az MI-rendszerek megfelelő és biztonságos használata kapcsán segítséget nyújthat továbbá az irányadó nemzetközi vagy ismertebb technikai előírásoknak, keretrendszereknek történő megfelelés, illetve ezek figyelembevétele. Ilyennek minősülhet például az amerikai NIST által kiadott „AI Risk Management Framework" elnevezésű, MI fejlesztésével, alkalmazásával kapcsolatos kockázatokra fókuszáló keretrendszer,[573] vagy a brit National Cyber Security Center által kiadott biztonságos MI fejlesztéssel foglalkozó, „Guidelines for secure AI system development" elnevezésű iránymutatások.[574] Az ezen iránymutatásoknak történő megfelelés azonban érthető módon nem helyettesítheti a jogszabályi megfelelést, illetve nem váltja ki a nagy kockázatú MI-rendszer megfelelő működésével kapcsolatos elszámoltathatóságot.

Kiemelendő, hogy az adatbiztonsági intézkedések kapcsán az MI Rendelet, valamint az adatvédelmi jogszabályok, mint a GDPR, jellemzően általánosnak tekinthető követelményeket határoznak meg, amelyek önmagukban nehezen alkalmazhatók,[575] így ennek kapcsán szükséges az adott tevékenységre vonatkozó speciális jogszabályi rendelkezések, szakmai iránymutatások, szervezetre vonatkozó sajátos követelmények figyelembevétele.

Az MI-rendszerekkel kapcsolatos adatbiztonsági követelmények tükrében az ilyen rendszereket érő esetleges adatvédelmi incidensek kezelése szintén kulcsfontosságúnak tekinthető. Informatikai környezetben az incidensek alatt számos, az adott rendszert vagy érintett információkat negatívan érintő esemény érthető. Ezzel szemben azonban az adatvédelmi incidensek körét szűkebben, akként határozza meg a GDPR mint „*a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi*".[576] A fentiek körébe értelemszerűen beletartozhatnak kifejezetten az MI-rendszerek fejlesztésével, alkalmazásával kapcsolatos, illetve az egyes MI-modelleket érő incidensek is, például a tanító adatkészleteket érő adatmérgezés (angolul: „*data*

[573] NIST, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework
[574] National Cyber Security Center, Guidelines for secure AI system development, https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
[575] KISS Attila: Információbiztonság és adatvédelem. Kapcsolódási pontok a hatályos és az EU adatvédelmi rendelete utáni szabályozásban. In: CZÉKMANN Zsolt (szerk.): *Infokommunikációs jog*. Budapest, Dialóg Campus Kiadó, 2019. 257.
[576] GDPR 4. cikk 12. pontja

poisoning") vagy a tanított modelleket érő ellenséges támadások (angolul: „*adversarial attacks*"), illetve az adott rendszer alapját képező infrastruktúrát érő támadások.[577]

Az adatvédelmi incidens azonosításán túl kiemelten fontos azonban annak megfelelő kategóriába sorolása is, tekintettel arra, hogy ezen meghatározás a megfelelő intézkedések meghozatala szempontjából is jelentőséggel bír. Ennek kapcsán az adatvédelmi incidensek alapvetően három kategóriába sorolhatók:

- titoksértés: személyes adatok jogosulatlan vagy véletlen közlése, illetve az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- sértetlenségi adatsértés: személyes adatok jogosulatlan vagy véletlen módosítása;
- hozzáférhetőségi adatsértés: személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése vagy az ilyen adatok véletlen vagy jogosulatlan megsemmisítése.[578]

Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, úgy szükséges azt bejelenteni az adatvédelmi felügyeleti hatóságnak,[579] amennyiben pedig ezen kockázat valószínűsíthetően magasnak tekinthető, úgy erről az érintettet is késedelem nélkül tájékoztatni kell.[580] Hangsúlyozandó, hogy amennyiben az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, úgy azt nem szükséges az adatvédelmi felügyeleti hatóság részére bejelenteni, vagy arról az érintetteket értesíteni, azonban szükséges az adatvédelmi incidenst az adatkezelőnek nyilvántartásba vennie.[581]

A gyakorlatban esetről-esetre vizsgálandó, hogy a valószínűsíthető kockázat fennáll-e, amely tekintetében az alkalmazott adatbiztonsági intézkedések köre kiemelt jelentőséggel bír. Így adott esetben a valószínűsíthető kockázat akár nagyobb számú vagy szenzitívebbnek tekinthető

[577] MI Rendelet (51) preambulum-bekezdés
[578] Adatvédelmi Munkacsoport 03/2014. sz. vélemény személyes adatok megsértése bejelentéséről, 693/14/EN, WP 213, elfogadva: 2014. március 25, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_hu.pdf. 5-6., Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, 18/HU, WP250rev.01, elfogadás időpontja: 2017. október 3., a legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6. https://ec.europa.eu/newsroom/article29/redirection/document/83862 („**Iránymutatás az Adatvédelmi Incidensek bejelentéséről**"), 8.
[579] GDPR 33. cikk (1) bek.
[580] GDPR 34. cikk (1) bek.
[581] GDPR 33. cikk (1), (5) bekezdései

adatkör esetén is alacsonynak tekinthető. Például, ha a személyes adatok archívumának biztonságos másolatát tároló USB-kulcsot ellopják, az adatvédelmi incidenst nem szükséges bejelenteni vagy arról az érintetteket tájékoztatni, feltételezve, hogy az adatokat a legkorszerűbb algoritmussal titkosítják, a titkosításhoz használt kulcsot az adatvédelmi incidens nem érintette, az adatok pedig kellő időben helyreállíthatók.[582] Így tehát, amennyiben az adott MI megoldás fejlesztéséhez használt adatokat tartalmazó adatbázishoz illetéktelenek férnek hozzá, azonban ezen adatok megfelelő adatbiztonsági intézkedésekkel (például federatív tanulással és homorfikus titkosítással) védettek, és erre tekintettel az érintettek és személyes adataik az illetéktelen személyek számára azonosíthatatlanok maradnak, úgy ennek kapcsán az érintettek jogaira és szabadságaira jelentett valószínűsíthető kockázat nem áll fenn, az adatvédelmi incidenst pedig nem szükséges bejelenteni az adatvédelmi hatóság részére, és nem szükséges arról az érintetteket sem tájékoztatni.

Az adatvédelmi incidensek megfelelő kezelése érdekében, amennyiben ez az adatkezelő által végzett adatkezelés tükrében arányos, az adatkezelőnek incidenskezelési szabályzatot szükséges készítenie,[583] amely meghatározza az adatvédelmi incidensek azonosításával és az azokra való megfelelő reagálással kapcsolatos lépéseket. Ennek részét képezi az adatvédelmi incidens egyéb incidensektől való elhatárolása is, amelyek kezelésére eltérő szabályok vonatkozhatnak (például: hírközlési szolgáltatókat, bankokat és pénzügyi szolgáltatókat érintő incidensek). Emellett az MI Rendelet megköveteli a nagy kockázatú MI-rendszerek élettartama során az ezek működésével kapcsolatos események automatikus rögzítését (naplózását),[584] illetve a súlyos váratlan események[585] bejelentését azon tagállam piacfelügyeleti hatóság számára, ahol ezen esemény történt.[586]

Kiemelendő, hogy az ilyen eseményről szóló értesítést a szolgáltatóknak haladéktalanul meg kell tenni azt követően, hogy a szolgáltató megállapította az MI-rendszer és a súlyos váratlan esemény közti ok-okozati összefüggést vagy az ilyen összefüggés észszerű valószínűségét, de legkésőbb 15 napon belül azt követően, hogy a szolgáltató, vagy ha ez releváns, az alkalmazó

[582] Iránymutatás az Adatvédelmi Incidensek bejelentéséről, 34.
[583] BH 2021.5.148. [18].
[584] MI Rendelet 12. cikk (1) bek.
[585] MI Rendelet 3. Cikk 49. Pontja értelmében súlyos váratlan eseménynek minősül "az MI-rendszernél fellépő olyan váratlan esemény vagy hibás működés, amely közvetlenül vagy közvetetten" valamely különösen súlyos következményhez vezet, ideértve valamely személy halálát, súlyos egészségkárosodást, kritikus infrastruktúrával kapcsolatos visszafordíthatatlan zavarokat, alapvető jogok védelmére irányadó uniós jog szerinti kötelezettségek megsértését vagy súlyos vagyoni vagy környezeti károsodást.
[586] MI Rendelet 73. cikk (1) bek.

az ilyen eseményről tudomást szerzett.[587] Ennek kapcsán megjegyzendő, hogy bizonyos különösen súlyos esetekben az MI Rendelet ennek rövidebb értesítési határidőket is rögzít (ideértve például haláleset esetén).[588] A bejelentés megtételét követően továbbá a szolgáltató köteles az eseménnyel, valamint az érintett rendszerrel kapcsolatos szükséges vizsgálatokat haladéktalanul elvégezni, amely magában foglalja az esemény kockázatértékelését, valamint korrekciós intézkedések megtételét.[589]

Az MI-rendszerek működésével kapcsolatos, illetve a fentiek szerinti súlyos váratlan események azonban nem feltétlenül minősülnek adatvédelmi incidensek. Így amennyiben például az adott esemény elhunyt személyek adatai kapcsán alkalmazott MI-rendszert érint, az – ennek kapcsán irányadó tagállami szabályozás hiányában – nem minősül adatvédelmi incidensnek, tekintettel arra, hogy ilyen adatok kapcsán átfogó európai szabályozásról nem, legfeljebb bizonyos szempontú tagállami követelményekről és a vonatkozó szolgáltatók sajátos szabályozási rendjéről beszélhetünk.[590] Megemlítendő továbbá, hogy amennyiben a fenti esemény egyben adatvédelmi incidensnek vagy egyéb jogszabály szerint bejelentendő, illetve kezelendő eseménynek is minősül, úgy a GDPR-ban, illetve az egyéb irányadó jogszabályi követelmények szerinti lépéseket is meg kell tenni (például: az adott incidens hatósági bejelentése, az érintettek tájékoztatása, kockázatcsökkentő intézkedések haladéktalan megtétele).

j. A szektorális adatkezelés kihívásai

Az MI általi adatkezeléssel kapcsolatos főbb kihívások számos esetben általános megközelítést és szabályozást követelnek meg. Ide tartoznak például az adatkezelés átláthatóságával, az adattovábbítások megfelelőségével, valamint az érintetti jogok gyakorlásának biztosításával kapcsolatos kihívások, amelyek az MI általi adatkezelés kapcsán számos esetben, illetve iparágban hasonlóan érvényesülnek. Emellett azonban bizonyos esetekben az MI általi adatkezeléssel kapcsolatos szektorális szempontok figyelembevétele különösen jelentősnek

[587] MI Rendelet 73. cikk (2) bek.
[588] MI Rendelet 73. cikk (3) – (4) bekezdések
[589] MI Rendelet 73. cikk (6) bek.
[590] Lilian EDWARDS, Edina HARBINJA: 'Be Right Back': What Rights Do We Have over Post-mortem Avatars of Ourselves? In: Lilian EDWARDS, Burkhard SCHAFER, Edina HARBINJA (eds.): *Future Law: Emerging Technology, Regulation and Ethics*. Edinburgh, Edinburgh University Press, 2020. 267.

mondható, az adott szakterület jellemzői pedig az MI általi adatkezelés sokszor különös szempontok szerinti értékelését követelik meg.

Habár a fentiek számos szakterület vagy tevékenység kapcsán elmondhatók, azonban bizonyos területeken az MI általi adatkezelés kapcsán különösen fontosnak tartottuk a szektorális szempontok, aggályok, illetve sajátos megközelítést követelő esetek ismertetését. Ennek kapcsán az alábbiakban az MI egészségügyi és munkahelyi alkalmazását, valamint az online platformokkal kapcsolatos MI általi adatkezelés sajátosságait ismertetjük, mivel ezen területeken az MI álláspontunk szerint kiemeltnek tekinthető társadalomformáló erővel bír, az adatvédelmi követelmények helyes érvényesítése pedig jelentős kihívást jelent.

i. A mesterséges intelligencia szerepe az egészségügyben

Az MI szerepe napjainkban számos területen jelentősnek mondható, az egészségügy területén azonban sok szempontból mégis kimagaslónak tekinthető. Az MI segítségével ugyanis mind az egészségügyi, mind a gyógyszerkutatások üteme és eredményessége jelentősen fokozható, továbbá számos folyamat automatizálható, a tevékenységellátás minősége pedig drasztikusan növelhető. Így például az MI hatékonyan lehet képes rákos elváltozások vagy más betegségek azonosítására, illetve klinikai vizsgálatok, kutatások támogatására.[591] Megemlítendő azonban, hogy az egyes betegségek azonosítása számos esetben kihívást jelenthet a technológia jelenlegi lépcsőfokán, tekintettel arra, hogy a betegségek azonosítására szolgáló megoldások túlérzékenysége vagy túlzott precizitása egyrészt számos téves diagnózishoz vezethet, és így a betegeket felesleges orvosi vizsgálatoknak teheti ki, míg másrészt a betegség számos esetben azonosítatlan maradhat, így veszélyeztetve az érintett betegek életét és egészségét.[592] Erre tekintettel értelemszerűen a fenti egészségügyi MI-rendszerek felülvizsgálata jellemzően nagyobb figyelmet követel meg a szolgáltatók részéről, mint más, kevésbé kockázatos rendszereké.

A fentieken túl az olyan megoldások, mint az egészségügyi vagy szociális robotok szintén jelentősen növelhetik a betegellátás hatékonyságát, adott esetben pedig segíthetik az

[591] Thomas DAVENPORT, Ravi KALAKOTA: The potential for artificial intelligence in healthcare. *Future Healthcare Journal*, 2019 Jun;6(2):94-98. doi: 10.7861/futurehosp.6-2-94. PMID: 31363513; PMCID: PMC6616181. 94.
[592] Hannah FRY: *Emberek és gépek. Hogyan tartsuk a kezünkben az irányítást a mesterséges intelligencia korában?* Budapest, HVG Kiadó Zrt, 2021. Fordította: Dembinszky Zsófia (2020), eredeti kiadás: 2018. 101.

egészségügyi személyzet munkavégzését is. A közeljövőben várhatóan további kihívásokat jelent majd az elveszett, illetve hiányzó vagy sérült emberi testrészek pótlása kiberfizikai rendszerekkel (angolul: „*Cyber-Physical Systems – CPC*”), amelyek kapcsán az adatbiztonság és a személyes adatok védelme egyben az emberi test fizikai integritásával és az egészség védelmével is összefüggést mutat.[593] Érdekes fejleménynek tekinthető, hogy nemrégiben a Neuralink nevű, Elon Musk techmilliárdoshoz köthető amerikai startup vállalkozás elsőként ültetett be agyi komputer chipet egy betegbe. A megoldás különös segítséget jelenthet például neurológiai betegségektől szenvedők, illetve mozgássérültek számára, de a vállalkozás hosszútávú céljai szerint akár számítógépes eszközöket is mozgathatnak majd az érintettek a gondolataikkal az implantátumnak köszönhetően.[594]

Az MI egészségügyi alkalmazása kapcsán azonban az innovatív megoldások keresésén túl az etikai elvárásoknak való megfelelés is kiemelten fontosnak tekinthető. Ez az MI-vel kapcsolatos általános etikai elvárásokon túl azonban a sajátos orvosi és egészségügyi szempontok figyelembevételét is megköveteli. Ennek kapcsán az egyik legismertebb amerikai orvosi szervezet („American Medical Association”; „**AMA**”) már évek óta jelentősebb figyelmet szentel az MI egészségügyi és kutatási célú felhasználásának. Így például az AMA „*Augmented Intelligence and Healthcare*” elnevezésű szabályzatában („**AMA Policy**”)[595] alapvető célkitűzéseket és követelményeket határozott meg az MI egészségügyi célú alkalmazásával kapcsolatban. E körbe tartozik például a megfelelő és átlátható, magas szintű egészségügyi MI megoldások fejlesztésén túl az egészségügyi MI megoldásokkal kapcsolatos képzés, valamint a megfelelő jogi környezet kialakítása is.[596] Emellett a dokumentum kiemeli annak fontosságát, miszerint az egészségügyi MI rendszerek szabályozásának és felügyeletének az adott megoldással kapcsolatos előnyök és hátrányok megfelelő értékelésén kell alapulnia, figyelembe véve – többek között – az adott megoldás szándékolt és észszerűen várható felhasználását, a biztonságos és hatékony, valamint igazságos felhasználással kapcsolatos bizonyítékok rendelkezésre állását, az automatizáció fokát, az átláthatóságot, valamint az alkalmazás feltételeit.[597]

---

[593] KLEIN Tamás: Robotok a beteggondozásban és a gyógyításban. In: KLEIN Tamás, TÓTH András (szerk.): *Technológia jog – Robotjog – Cyberjog*. Budapest, Wolters Kluwer Hungary, 2018. 211.
[594] Reuters, Elon Musk's Neuralink implants brain chip in first human, 2024.01.30, https://www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/
[595] AMA, Augmented intelligence in healthcare, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf
[596] AMA Policy, Foundational policy Annual 2018. 1.
[597] AMA Policy, Regulation, payment, liability and other key policies Annual 2019. 2.

Emellett kiemelendők az AMA egészségügyi MI megoldások alkalmazásával kapcsolatos felelősségre vonatkozó meglátásai. Így az AMA az adott megoldás tervezése és fejlesztése során a fejlesztő felelősségét, valamint egyes szempontokból az eljáró orvos felelősségét tartja hangsúlyosnak (például: alkalmazás megfelelő orvosi céljának meghatározása, a megfelelő működés biztosítása), míg a megoldás alkalmazása és felügyelete során már az azt alkalmazó szervezet vagy személyek, illetve az eljáró orvos felelősségét emeli ki. Kiemelendő azonban, hogy az esetek döntő többségében az AMA az eljáró orvos felelősségét hangsúlyozza, így a jövőben vélhetőleg kiemelt szerepet kap majd az orvosi képzésben, valamint a gyakorlati időszak során az egészségügyi MI rendszerek alkalmazásának, felügyeletének megfelelő elsajátítása, valamint az ilyen rendszerekkel való együttműködés, ezekhez való alkalmazkodás.[598]

Az MI egészségügyi alkalmazása kapcsán az érintettek tájékoztatása különösen fontosnak tekinthető, ugyanis az ilyen adatkezelés jellemzően sérülékeny érintetti csoportokat (például: betegek, idősek, gyermekek, fogyatékos személyek) érint, akik adott esetben kevésbé képesek átlátni személyes adataik kezelését. Emellett az MI-rendszerek által végzett adatkezelési műveletek jellemzően kifejezetten összetettnek mondhatók, amelyek tovább növelik az adatkezelés átláthatóságával kapcsolatos kihívásokat. Így az adatkezelőnek különös gondot kell fordítania az érintettek által érthető, megfelelő adatvédelmi tájékoztató elkészítésére, illetve az adatkezelés átlátható folytatására és az érintetti jogok gyakorlásának támogatására. Kiemelendő azonban, hogy az MI technológiai sajátosságai okán, akár egészségügyi szolgáltatás, akár kutatási célú adatkezelés esetén jellemzően előre nem jósolható meg sem az MI által hozott valamennyi lehetséges döntés, sem az adatok valamennyi lehetséges jövőbeli felhasználása.[599] Így amennyiben egy radiológiai felvétel elemzése alapján az MI arra a következtetésre jut, hogy az érintettnél rákos megbetegedés diagnosztizálható, az orvos, vagy a rendszert biztosító szolgáltató vagy az azt felügyelő informatikai szakember sem lehet feltétlenül képes arra, hogy pontos magyarázatot adjon az MI fenti következtetésére.[600] Ettől függetlenül azonban a megfelelő további vizsgálatokkal és orvosi szakvéleménnyel az MI által levont következtetés

[598] AMA, Advancing health care AI through ethics, evidence and equity, https://www.ama-assn.org/practice-management/digital/advancing-health-care-ai-through-ethics-evidence-and-equity
[599] Mirko FORTI: The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR. *European Journal of Legal Studies* 13 (1). (2021), https://ssrn.com/abstract=3866576. 35.
[600] DAVENPORT, KALAKOTA op. cit. 97.

vagy kimutatott eredmény tovább pontosítható, illetve annak kapcsán az orvos már képes lehet további magyarázat szolgáltatására, amely az MI döntési mechanizmusának és alapvető működési szempontjainak ismertetésével, valamint az adott rendszer folyamatos felülvizsgálatával és ellenőrzésével kellő szintű átláthatóságot biztosíthat a rendszer egészségügyi alkalmazása kapcsán.

Az MI-rendszerek egészségügyi alkalmazása esetén az érintett hozzájárulása is sok esetben sajátos módon foghat helyt, amely kapcsán a jogirodalomban is többféle álláspont jelent meg, e körbe értve például az ún. dinamikus hozzájárulást, amely értelmében a betegek egy interfészen vagy más hasonló felületen keresztül aktív módon kommunikálhatnak az egészségügyi vagy kutatói személyzettel.[601] Emellett kontextuális hozzájárulásról is beszélhetünk, ahol a hozzájárulás továbbra is központi kérdés marad, azonban az egészségügyi környezet, valamint a technológia által indokolt módon, és ezen körülményekre tekintettel a hozzájárulás kezelésének folyamata során alakítható.[602] Mindezen hozzájárulással kapcsolatos megközelítések álláspontunk szerint elgondolkodtató alternatívát jelentenek a lineáris folyamatként tekintett, „klasszikus értelemben vett" hozzájáruláshoz viszonyítva, amelynek során az érintett egyszeri alkalommal megadja a hozzájárulást, amely a hozzájárulás visszavonásáig vagy az adatkezelés céljának megszűnéséig azonos tartalommal és feltételekkel marad releváns. Ezen statikus megközelítés álláspontunk szerint az MI általi adatkezelés egyéb eseteiben sem feltétlenül adhat naprakész választ a hozzájárulás megfelelő kezelésére, az egészségügyi környezet által, a betegek egészsége és érdekeinek védelme érdekében megkövetelt gyors döntéshozatal azonban a hozzájárulás „rugalmasabb" módon történő kezelését még inkább indokolttá teszi. A hozzájárulás e körben történő dinamikus értelmezése így adott esetben még szélesebb jogérvényesítést lehetőségeket biztosíthat a beteg vagy a nevében eljáró képviselője számára, és a változó, sokszor technikai környezetben történő jogérvényesítést is megkönnyítheti, például: egy kórházi robot vagy szoftver által lejátszott hangfelvétel, vagy az adatkezelés újabb szakaszairól küldött emlékeztető útján.[603]

[601] Jane KAYE, Edgar A WHITLEY, David LUND, Michael MORRISON, Harriet TEARE, Karen MELHAM: Dynamic consent: a patient interface for twenty-first century research networks. *European Journal of Human Genetics*, 2015. https://doi.org/10.1038/ejhg.2014.71. 141.
[602] Carina DORNECK, Ulrich M. GASSNER, Jens KERSTEN, Josef Franz LINDNER, Kim Philip LINOH, Katja NEBE, Henning ROSENAU, Birgit SCHMIDT AM BUSCH: Contextual Consent – Selbstbestimmung diesseits der Illusionen des Medizinrechts, *Medizinrecht*, 2019/37. https://doi.org/10.1007/s00350-019-5247-2. 432.
[603] Eduard FOSCH-VILLARONGA: Robots, Healthcare, and the Law. Regulating Automation in Personal Care, e-book version, 2020. 181–182.

Természetesen a fentieken túl a megfelelő adatbiztonsági intézkedések alkalmazása sem hanyagolható el, különösen az egészségügyi célú adatkezelések által érintett adatok szenzitív jellegére, az érintettek gyakori kiszolgáltatottságára. Így, különösen a nagy számú betegadatot MI-rendszerek alkalmazásával kezelő szervezetektől elvárható a szükséges szervezési és technikai intézkedések körének felmérése, valamint az irányadó jogszabályi rendelkezéseken túl, a szakmai és etikai iránymutatásoknak megfelelő alkalmazása, továbbá azok folyamatos felülvizsgálata.

ii. A mesterséges intelligencia munkahelyi alkalmazása

Az MI a fentebb írtakon túl a munkahelyeket és a munkához való viszonyunkat is forradalmasítja, illetve új alapokra helyezi. Segítségével ugyanis rengeteg időigényes vagy monoton feladat könnyebben elvégezhető, emellett azonban számos, korábban emberek által betöltött pozíciót is feleslegessé tesz. Ezek napjainkban akár komplexebb feladatok elvégzését megkívánó munkaköröket is magukban foglalhatnak, de előfordulhat, hogy a technológia fejlődése egy adott szakma karrierívének alján elhelyezkedő feladatok elvégzését teszi automatizálhatóvá, amely egyben a junior pozíciókat is veszélyeztetheti (például: gyakornoki feladatok elvégzését, illetve a jogi szakma esetén akár az ügyvédjelölti vagy kezdő ügyvédi munkát is),[604] miközben, jellemzően a technológiai területen eljáró tanácsadók (ideértve adott esetben úgyszintén az ügyvédeket) esetén az MI fejlődése egyre gyorsuló ütemben követeli meg a szakmai tudás naprakészen tartását.[605] Emellett továbbá általánosságban is elmondható, hogy nem kizárólag a munkaerő kiváltását, helyettesítését vonja maga után az MI fejlődése, hanem bizonyos körben egyes készségek, képességek kialakítását is nélkülözhetővé teheti, amelyek szükségesek a megfelelő alkalmazkodóképesség és intelligencia kialakításához.[606] Így a társadalom egyre nagyobb rétegjei szorulhatnak fokozott mértékben az MI támogatására, akár a napi munkájuk során, akár az élet más területein.

Emellett az MI alkalmazása diszkriminációs problémákhoz is vezethet, ugyanis a nem megfelelő minták alapulvétele és a nagyfokú automatizáció révén az MI bizonyos személyekre

[604] Hannah ROBERTS: Is The Rise in AI Use Damaging Junior Lawyers' Skills. *Law.com International*, 2020.07.13, https://www.law.com/international-edition/2020/07/13/is-the-rise-in-ai-use-damaging-junior-lawyers-skills/?slreturn=20230725124725
[605] Deepa RAVINDRANATH: A Guide to Commercial Innovation in Artificial Intelligence. *Les Nouvelles - Journal of the Licensing Executives Society*, vol. 52. no. 4. (September 2017), https://ssrn.com/abstract=3009423. 237.
[606] Marketa TRIMBLE: Artificial Intelligence and Human Intelligence. *GRUR International*, vol. 72., issue 1. (January 2023). https://doi.org/10.1093/grurint/ikac109. 1.

vagy meghatározott társadalmi csoportokra nézve hátrányosabb döntéseket hozhat. Így például, amennyiben a jelentkezők kiválasztását segítő MI-rendszer fejlesztéséhez a korábbi kiválasztásokra vonatkozó tanító adatokat vesznek alapul, ez könnyen társadalmi igazságtalanságok bebetonozásához, diszkriminatív gyakorlatok felerősítéséhez vezethet.[607] A fentiekre tekintettel aggályokra adhat okot továbbá az az immáron számos vállalat esetén megjelenő gyakorlat, amely tükrében MI-rendszer hoz meg a munkaviszony szempontjából kritikus döntéseket, ideértve például a munkaviszony megszüntetését is. A Worker Info Exchange nevű szervezet például 2023. áprilisában tett közzé egy jelentést a Just Eat ételfutárcég azon gyakorlatáról, amely szerint a cég a futárok elbocsátásáról sok esetben automatizált döntéshozatal útján rendelkezett.[608] Ahogy tehát a fentiekből is látszik, az MI és az automatizációs megoldások gyökeresen alakítják át a munkaerőpiacot,[609] amely egyúttal a munkavállalók személyes adatainak kezelésére is hatással van.

A fentiek kapcsán az EU-n belül a GDPR korlátozza azon eseteket, amikor az érintettre joghatással járó, vagy őt hasonlóképpen jelentős mértékben érintő döntéseket automatizált döntéshozatal útján hoznak meg.[610] Emellett a GDPR további korlátozásokat alkalmaz a fenti döntések meghozatalával kapcsolatban, valamint az érintettek számára megfelelő jogokat biztosít, amelyeket a fenti, érintetti jogok gyakorlásáról szóló fejezetben ismertettünk. További hasznos fejleménynek tekinthetők a tervezett, platformalapú munkavégzés munkakörülményeinek javításáról szóló irányelvjavaslat („**Irányelvjavaslat**”) rendelkezései,[611] amelyek különösen az automatizált nyomonkövetési és döntéshozatali rendszerek átláthatósága és használata kapcsán írnak elő alapvető követelményeket. Ezen követelmények azért is tekinthetők jelentősnek, mivel a platformalapú munkavégzés és az algoritmusalapú technológiák számos szektorban (például: közlekedés, ételkiszállítás, egyes szolgáltatások) dominánssá váltak, számos esetben megkönnyítve a szolgáltatást keresők összekötését az egyes szolgáltatásokat nyújtó vagy abban résztvevő személyekkel.[612]

---

[607] Shlomit YANISKY-RAVID, Sean HALLISEY: ‘Equality and Privacy by Design’: Ensuring Artificial Intelligence (AI) Is Properly Trained & Fed: A New Model of AI Data Transparency & Certification As Safe Harbor Procedures, 2018.11.05, https://ssrn.com/abstract=3278490, http://dx.doi.org/10.2139/ssrn.3278490. 16.
[608] Worker Info Exchange, Just Beat It! How Just Eat Robo-fires its Workers, April 2023, https://www.workerinfoexchange.org/just-eat-report. 1.
[609] HAJDÚ József: A mesterséges intelligencia hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját. *Infokommunikáció és jog*, 2020/2. 5.
[610] GDPR 22. cikk (2) bek.
[611] Javaslat, az Európai Parlament és a Tanács irányelve a platformalapú munkavégzés munkakörülményeinek javításáról, Brüsszel, 2021.12.9. COM(2021) 762 final, 2021/0414(COD).
[612] TÓTH András: Az online platformok európai szabályozása. *In Medias Res*, 2022/2. 84. [a továbbiakban: TÓTH (2022)].

Erre tekintettel az Irányelvjavaslat értelmében a tagállamok kötelesek előírni a digitális munkaplatformok számára a platform-munkavállalóik tájékoztatását az ezen személyek munkateljesítményének elektronikus úton történő nyomon követésére, felügyeletére vagy értékelésére használt automatizált nyomonkövetési rendszerekről, valamint a platform-munkavállalók munkakörülményeit jelentősen befolyásoló automatizált döntéshozatali rendszerekről.[613] Ezen tájékoztatásnak szükséges kiterjednie az automatizált nyomonkövetési rendszerek tekintetében a rendszer használatának, illetve bevezetésük folyamatban létének tényére, továbbá a rendszer által nyomon követett, felügyelt vagy értékelt tevékenységek kategóriáira,[614] az automatizált döntéshozatali rendszerek tekintetében pedig az alkalmazásuk vagy bevezetésük folyamatban létének ténye mellett a rendszerek által meghozott vagy alátámasztott döntések kategóriáira, a rendszerek által figyelembe vett fő paraméterekre és ezek relatív jelentőségére az automatizált döntéshozatalban, valamint a platform-munkavállaló munkavégzésére, jogviszonyára vonatkozó jelentős döntések indokaira (ideértve például: fiók felfüggesztése, javadalmazás megtagadása).[615] A tájékoztatást legkésőbb az első munkanapon, valamint jelentős változások esetén kérésre bármikor rendelkezésre kell bocsátani (akár elektronikus dokumentumban is).[616]

Az Irányelvjavaslat megtiltja továbbá az olyan személyes adatok kezelését a platform-munkavállalókról, amelyek nem kapcsolódnak szorosan a velük kötött szerződés teljesítéséhez, és ahhoz nem feltétlenül szükségesek. Ezen belül az Irányelvjavaslat külön is megtiltja a platform-munkavállalók érzelmi és pszichológiai állapotára vonatkozó személyes adatok, a foglalkoztatáshoz szükségtelen körben az egészségügyi adatok, valamint a személyes beszélgetésekkel kapcsolatos személyes adatok kezelését, valamint a platformalapú munkán kívüli személyes adatok gyűjtését,[617] ezáltal a diszkrimináció lehetőségét, a platform-munkavállalók kihasználását, adataik szükségtelen körű kezelését korlátozva.

A fentiek mellett az Irányelvjavaslat az automatizált nyomonkövetési és döntéshozatali rendszerek által hozott vagy alátámasztott egyedi döntések munkakörülményekre gyakorolt hatásának nyomon követését és értékelését, megfelelő munkavédelmi intézkedések

[613] Irányelvjavaslat, 6. cikk (1) bek.
[614] Irányelvjavaslat, 6. cikk (2) bek. a) pontja
[615] Irányelvjavaslat, 6. cikk (2) bek. b) pontja
[616] Irányelvjavaslat, 6. cikk (3) bek.
[617] Irányelvjavaslat, 6. cikk (5) bek.

alkalmazását is elvárja a digitális munkaplatformoktól,[618] továbbá a platform-munkavállalóknak jogokat biztosít arra, hogy magyarázatot kérjenek a platform-munkavállaló munkakörülményeit jelentős mértékben befolyásoló, automatizált döntéshozatali rendszer által hozott vagy alátámasztott döntésekről,[619] továbbá, ha nem elégedettek a döntésről kapott magyarázattal, illetve indokolással, illetve úgy ítélik meg, hogy az jogaikra sérelmes, jogosultak kérni a digitális munkaplatformtól a döntés felülvizsgálatát.[620] Az érintett platform-munkavállaló jogait sértő döntést haladéktalanul helyesbíteni kell, vagy ha ez nem lehetséges, megfelelő kártérítést kell nyújtani.[621]

Hangsúlyozzuk, hogy habár az Irányelvjavaslat szövege még nem tekinthető véglegesnek, az abban foglaltak mindenképp fontos előrelépést jelentenek a platform-munkavállalók (ideértve a munkaviszonytól eltérő jogviszonyban foglalkoztatott személyeket is)[622] jogainak védelme érdekében, számos szektorban támogatva a hatékony önfoglalkoztatás kereteit és lehetőségét.[623] Érdemes megemlíteni továbbá, hogy a nyomonkövetési és döntéshozatali rendszerek munkaviszonyban történő alkalmazására már felfigyeltek az adatvédelmi hatóságok az EU-n belül. Így például 2021-ben az olasz adatvédelmi hatóság egy ételkiszállító társaságot büntetett a társaság automatizált pontozási rendszere miatt, amely átláthatatlan, illetve diszkriminatív módon kínált lehetőségeket a futárok részére, aránytalanul, megfelelő magyarázat nélkül kizárva egyes futárokat a megrendelésekből.[624]

Megemlítendő, hogy az Egyesült Államokban – az amerikai MI szabályozás kapcsán írt fejezetünkkel összhangban – az MI munkahelyi alkalmazásával kapcsolatos szabályozás főleg a tagállami szabályozás szintjén tekinthető jelentősnek. Így például több tagállam is vezetett már be automatizált toborzási eszközökkel kapcsolatos szabályozást a fentebb írtak szerint. Az amerikai szabályozás az MI-rendszerek toborzási, valamint munkahelyi alkalmazása során jelentős hangsúlyt helyez a munkahelyi diszkriminációra, illetve az az elleni küzdelemre, amely

[618] Irányelvjavaslat, 7. cikk
[619] Irányelvjavaslat, 8. cikk (1) bek.
[620] Irányelvjavaslat, 8. cikk (2) bek.
[621] Irányelvjavaslat, 8. cikk (3) bek.
[622] Ennek kapcsán megemlítendő, hogy a fenti követelmények a platformalapú munkát végző személyekre abban az esetben is irányadók, ha azok nem rendelkeznek munkaszerződéssel vagy munkaviszonnyal (lásd: Irányelvjavaslat 10. cikk (1) bek.), annak érdekében, hogy azok ne legyenek megkerülhetők vagy kijátszhatók az egyes platformok szolgáltatói részéről.
[623] TÓTH (2022) i.m. 100-101.
[624] Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021 [9685994], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994

az MI-rendszerek alkalmazása esetén a gyakorlatban jelentős kihívást jelenthet, tekintettel arra, hogy az MI-rendszerek általi döntéshozatal jellemzően meghatározott mintákat vesz alapul, és ennek alapján dönt például egy munkavállaló felvételéről, előléptetéséről vagy elbocsátásáról. Az irányadó New York-i jogszabály ennek kapcsán például a vonatkozó toborzási célú MI-rendszerek kapcsán elfogultsági ellenőrzés („*bias audit*") elvégzését írja elő legalább évente, amellyel az automatizált döntéshozatal során érvényesülő diszkrimináció csökkenthető.[625]

A toborzás mellett természetesen egyre jelentősebb szerepet játszik az MI a munkahelyi ellenőrzés kapcsán is (például: internet- és email fiók használat ellenőrzése). Ennek során azonban a munkáltatónak tiszteletben kell tartania a munkavállaló személyiségi jogait, ideértve a személyes adatai védelméhez fűződő jogát is. Az EJEB is kiemelte a Bărbulescu v. Románia ügyben, miszerint a munkahelyi internethasználat szankciós célú eseti ellenőrzése jelentősen sértheti a munkavállalók személyes adatok védelméhez fűződő jogát. Erre tekintettel a munkáltatók a munkahelyi ellenőrzés során arányosan, a fokozatosság elve szerint kötelesek eljárni.[626] Így jellemzően jogsértőnek minősül, ha a munkáltató a munkavállaló teljes munkahelyi internethasználatát ellenőrzi, valamennyi látogatott weboldal és letöltés megtekintésével, figyelemmel arra, hogy egy ilyen átfogó, teljeskörű ellenőrzés jelentősen és aránytalan módon korlátozza a munkavállaló személyiségi jogait.[627] Arányosnak tekinthető azonban, ha a munkáltató például fokozatos lépések útján, indokolt esetben (például: jogsértés gyanúja, közérdekű bejelentést követő vizsgálat) ellenőrzi a munkavállaló internet-, informatikai eszköz-, illetve e-mail fiók használatát. Ez esetben is azonban a jogsértés megállapítása vagy kizárása érdekében fokozatos intézkedéseket szükséges alkalmaznia. A munkáltatónak továbbá a munkahelyi internethasználat biztosítása és szabályozása során is ajánlott olyan intézkedéseket hoznia, amelyek mind az esetleges jogsértéseket és visszaéléseket, mind az ellenőrzés szükségességére alapot adó esetek számát csökkentik (például: kockázatos weboldalak hozzáférhetőségének korlátozása).[628] Megemlítendő továbbá, hogy az internet- és eszközhasználat megfigyelésén túl a munkavállalókról kamera-, illetve hangfelvételek készítése is csak szükséges esetben, az érintettek jogaival arányosan foghat helyt, amely nem vezethet a munkavégzés minőségének ellenőrzéséhez. Így például

[625] NY Local Law 144, § 5-301
[626] Bărbulescu v. Romania, no. 61496/08., 2017. szeptember 5-i ítélet, 121, 131, 133. bekezdések
[627] Adatvédelmi Munkacsoport 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról, 844/14/HU, WP 217, elfogadás időpontja: 2014.04.09, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf. 69.
[628] Uo.

Magyarországon a NAIH egy szépségközpont üzemeltetőjével szembeni eljárás során megállapította, miszerint a munkavállalók folyamatos megsértésével, valamint a munkavállalók pihenés céljára szolgáló helyeinek megfigyelésével a munkáltató kifejezetten megsértette a tisztességes adatkezelés alapelvét.[629]

Kiemelendő továbbá, hogy amennyiben a munkáltató MI-rendszert alkalmaz a munkahelyen rendszerei, eszközei védelme érdekében, úgy a kapcsolódó adatkezelés céljának is a munkáltató hálózatának, rendszereinek, valamint az azon tárolt információknak a védelme kell, hogy legyen, nem pedig a munkavállaló szankcionálása vagy a munka minőségének ellenőrzése. Amennyiben azonban egy esetleges jogvita, hatósági eljárás, bejelentés vagy panasz kivizsgálása szükségessé teszi MI alapú vagy más hasonló megoldás alkalmazását (például: a munkáltatóval szembeni peres eljárás vagy hatósági vizsgálat kapcsán többezer e-mail átvizsgálása válna szükségessé), úgy a munkáltatónak az alkalmazás során elsődlegesen a jogsértő esetek kiszűrésére kell fókuszálnia, mielőtt az érintett azonosítására, illetve vizsgálat alá vonására kerülne sor.

iii. A mesterséges intelligencia alkalmazása az online platformokon

Napjaink digitális gazdaságában a platformok kialakulása és elterjedése meghatározóvá vált. A platformok jelentős részének működése (ideértve például a közösségi médiaoldalakat vagy keresőszolgáltatásokat) az ún. zéró-áras üzleti modellen alapul, amelynek értelmében a felhasználók nem fizetnek a szolgáltatásért, azonban jelentős mennyiségű személyes adatot adnak meg a platform használata során, amelyet a platform üzemeltetője hirdetések kínálása és kapcsolódó analitikai folyamatok végzése érdekében használ fel.[630] Így a felhasználók száma és az általuk végzett interakciók mennyisége egyre több hirdetőt vonzz a felületre, amely a hirdetésekből származó bevételek növelése érdekében igyekszik minél inkább lekötni a felhasználók figyelmét, amely révén egyre nagyobb mennyiségben, és jellemzően egyre szofisztikáltabb módon kerül sor személyes adatok kezelésére is.[631] Ennek kapcsán látható, hogy az MI a platformgazdaság, valamint az adatok hatékonyabb felhasználásának területén jelentős szerepet tölt be. Az MI szerepe a közösségi médiaoldalakon kiterjed például a

[629] NAIH-2732-2/2023. sz ügyben hozott határozat. [141]. 23.
[630] TÓTH András: Az ingyenesség állítása mint fogyasztóvédelmi kihívás a digitális gazdaságban. In: RIGÓ Csaba Balázs, SZOBOSZLAI Izabella, CSIRSZKI Martin Milán (szerk.): *A hazai fogyasztóvédelmi jog áttekintése: alapok, kihívások, aktualitások*. Budapest, Gazdasági Versenyhivatal, 2023. 259.
[631] TÓTH (2018) i.m. 51.

tartalomgyártásra, a tartalomszabályozásra- és moderálásra, valamint a marketingkampányok menedzselésére és a brand-védelemre.[632] Az MI segítségével hatékonyabb elemezhetők a felhasználók szokásai, dinamikusan értékesíthetők az egyes hirdetési helyek, valamint könnyebben ismerhetők fel és távolíthatók el a nem megengedhető tartalmak. A C-446/21. sz. Maximilian Schrems kontra Meta Platforms Ireland Limited ügyben az EUB – többek között – azt a kérdést vizsgálta, hogy olyan személyes adatok, amelyekkel a Facebook vagy más hasonló platform rendelkezik, személyre szabott hirdetések céljából időbeli és az adatok típusa szerinti korlátozás nélkül összesíthetők, elemezhetők és kezelhetők-e. Ennek során az adatok kezelésének időbeli és adatok jellegétől függő korlátozása tekintetében való döntést a főtanácsnok az eljáró bíróságra bízta, tekintette arra, hogy e tekintetben az ügy körülményeire tekintettel hozható döntés.[633] Hangsúlyozta azonban az „aktív" (például: lájkolás) és a „passzív" (például: egy oldal puszta látogatása) felhasználói magatartás közti különbséget, valamint az érintettek észszerű magatartásának figyelembevételét.[634] Mindezeket figyelembevéve a főtanácsnok arra a megállapításra jutott, hogy a személyes adatokat személyre szabott hirdetések céljából időbeli és az adatok típusa szerinti korlátozás nélküli kezelése ellentétes az adattakarékosság elvével.[635] Erre tekintettel tehát az adott platform nem kezelheti a platformon elérhető valamennyi adatot korlátozás nélkül hirdetési, illetve kapcsolódó analitikai célból, szükséges e tekintetben arányos korlátozásokat alkalmaznia (például: elavult információk figyelmen kívül hagyása), illetve az érintett döntéseit és észszerű elvárásait is tiszteletben tartania.

Ahogy azt a fentiekből is láthatjuk, az MI platformokon történő alkalmazásával kapcsolatban az egyik legjelentősebb kritika általában tartalmak ajánlásához, szűréséhez, analitikai műveletek végzéséhez használt algoritmusokat éri. Ez kiterjedhet az egyes tartalmak felhasználók számára, célzott módon való megjelenítésére, a tartalmak szűrésére es korlátozására, akár az azt közzétevő felhasználók tudta nélkül is. Mindez értelemszerűen számos jogi es etikai aggályt is felvet, ideértve adott esetben a diszkriminatív tartalomszűrést, figyelembe véve, hogy az algoritmusok gyakran fejlesztőik meglévő nézeteit, előítéleteit hordozzák, amelyek igy az MI automatizált gyakorlata útján átfogó, diszkriminatív gyakorlat

[632] Rem DARBINYAN: How AI Transforms Social Media. *Forbes*, 2023.03.16, https://www.forbes.com/sites/forbestechcouncil/2023/03/16/how-ai-transforms-social-media/
[633] Ranthos főtanácsnok indítványa C-446/21. sz. ügyben, 22. és 23. pontok
[634] Ranthos főtanácsnok indítványa C-446/21. sz. ügyben, 25. és 26. pontok
[635] Ranthos főtanácsnok indítványa C-446/21. sz. ügyben, 28. pont

kialakításához vezethetnek.[636] A fenti gyakorlat révén bizonyos kissebségekhez vagy államok polgáraihoz kötődő tartalmak korlátozásra kerülhetnek, illetve meghatározott politikai vagy egyéb narratívák válhatnak túlsúlyossá, anélkül, hogy az érintettek ezzel tisztában lehetnének. Adatvédelmi szempontból a fentiek mellett az egyes platformok, közösségi médiaoldalak hirdetési, tartalommegjelenítési gyakorlata is adott esetben aggályosnak tűnhet, tekintettel arra, hogy az adott platform a felhasználók számára kevéssé átlátható módon korlátozhat vagy épp helyezhet előtérbe bizonyos tartalmakat.[637] Mindez fogyasztók esetén a döntéshozatal befolyásával is járhat, így adott esetben a nagyobb marketing büdzsével rendelkező vállalkozások tartalmai hamarabb juthatnak el a fogyasztókhoz, mint a helyi kisvállalkozások által megosztott tartalmak.

A fenti problémák kapcsán megoldást jelenthet az algoritmusok alkalmazását megelőző átfogó hatásvizsgálat elvégzése, valamint az algoritmusok működésének folyamatos figyelemmel kisérése az esetleges diszkriminatív minták kiszűrése érdekében. Emellett szinten fontos szempontot képez a nagyobb fokú átláthatóság megkövetelése, amely kiterjed az adott megoldás által alkalmazott logika es döntési mechanizmus átfogó bemutatására a felhasználók részére, ideértve az arra kiterjedő magyarázatot is, hogy a felhasználók döntései hogyan befolyásolják a tartalmak részükre való megjelenítését vagy az általuk előállított tartalmak más felhasználók számára való elérhetőségét.

Az utóbbi időszakban jelentős fejleményeket könyvelhetett el az EU platformszabályozása, amely az MI-rendszerek alkalmazására is hatással bír. Az EU online platformokkal kapcsolatos szabályozása azonban, tekintettel arra, hogy különböző szabályozandó tárgykörök mentén fejlődött, igy napjainkra széttagoltan létezik, a vonatkozó joganyag pedig gyakran eltérő definíciós készlettel dolgozó, es nehezen áttekinthető.[638] Ez alól – az MI vonatkozásában – a különböző ajánló- és értékelőrendszerekkel, profilalkotással kapcsolatos szabályok sem jelentenek kivételt, így bár valamennyi jogszabály jellemzően hivatkozik a GDPR – általában a tájékoztatással, hozzájárulással, érintetti jogokkal, profilalkotással kapcsolatos – rendelkezéseire, a szabályok megfelelő összhangja több szempontól is kérdéses marad. Mindezt

[636] Annie BROWN: Understanding The Technical And Societal Relationship Between Shadowbanning And Algorithmic Bias. *Forbes*, 2021.10.27, https://www.forbes.com/sites/anniebrown/2021/10/27/understanding-the-technical-and-societal-relationship-between-shadowbanning-and-algorithmic-bias/
[637] KOLTAY András: Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása. Budapest, Wolters Kluwer Hungary Kft., 2019. 204. [a továbbiakban: KOLTAY (2019)]
[638] TÓTH (2022) i.m. 79.

csak erősíti az a tény, hogy a platformjogi szabályok többségé formális, eljárási jellegű marad, a tartalmi kritériumok kidolgozását, érvényesítését a szabályozás így alapvetően a platformokra bízza,[639] amelyek jellemzően üzleti szempontokat érvényesítenek.

A fentiek kapcsán jelentős fejleménynek tekinthetők a digitális szolgáltatásokról szóló rendelet („**DSA**")[640] követelményei, amelyek különösen az online platformokon alkalmazott ajánlórendszerekkel, valamint azok átláthatóságával kapcsolatosan állapítanak meg szabályokat.[641] A DSA értelmében azon online platformot üzemeltető szolgáltatóknak, akik online interfészükön hirdetéseket jelenítenek meg, a szolgáltatások igénybe vevői számára szükséges világos, tömör, egyértelmű és valós idejű tájékoztatást nyújtaniuk a hirdetés tényéről, a hirdető és a finanszírozó személyéről, valamint a szolgáltatás hirdetéssel megcélzott igénybe vevőjének meghatározására szolgáló paraméterekkel kapcsolatos érdemi információkról, és arról is, hogy adott esetben hogyan lehet módosítani ezen paramétereket.[642] Ennek tükrében tehát az online platformon megjelenő hirdetések kapcsán szükség az érintettek számára például arról is tájékoztatást nyújtani, hogy az érintett milyen paraméterek alapján került meghatározásra egy csoport részeként (például: fiatal felnőttek, nyugdíjas felhasználók). Hangsúlyozandó továbbá, hogy az online platformot üzemeltető szolgáltató nem jeleníthet meg profilalkotáson alapuló hirdetéseket különleges adatok (például politikai véleményre, vallási meggyőződésre vonatkozó információk) felhasználásával.[643] Mindez azért is fontos, mivel ezen tulajdonságok felhasználása az érintettek viselkedését, döntési kompetenciáját is jelentős módon befolyásolhatja.

Hangsúlyozandó továbbá, hogy azon online platformot üzemeltető szolgáltatóknak, amelyek ajánlórendszereket használnak, általános szerződési feltételeikben meg kell határozniuk ezen ajánlórendszerekben foglalt fő paramétereket is, valamint a szolgáltatás igénybe vevői által ennek módosítására vagy befolyásolására rendelkezésre álló lehetőségeket.[644] A fő paramétereknek továbbá magyarázatot kell adniuk arra, hogy miért ajánlják az adott

[639] ZŐDI Zsolt: Az európai platformszabályozás jellegzetességei. Platformjog és felhasználóvédelem. *In Medias Res*, 2022/1. 81. [a továbbiakban: ZŐDI (2022)]
[640] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (EGT-vonatkozású szöveg), PE/30/2022/REV/1, HL L 277., 2022.10.27, p. 1–102 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[641] Lásd különösen: DSA 27, 38, 39. cikkei
[642] DSA 26. cikk (1) bek.
[643] DSA 26. cikk (3) bek.
[644] DSA 27. cikk (1) bek.

információkat a szolgáltatás igénybe vevője számára, e körbe értve az ilyen információk meghatározása szempontjából legjelentősebb kritériumokat, illetve a paraméterek viszonylagos fontosságának okait.[645] Amennyiben pedig több opció is rendelkezésre áll a szolgáltatás igénybe vevői számára megjelenített információk relatív sorrendjét meghatározó ajánlórendszerek tekintetében, úgy olyan funkció hozzáférhetővé tétele is szükséges, amelynek segítségével az érintett kiválaszthatja vagy módosíthatja az általa előnyben részesített opciót.[646] E körben a szolgáltatók moderálási tevékenysége is szerepet játszhat, amely során a kártékony vagy manipulatív tartalmak, ilyen tartalmak megosztása céljából létrehozott fiókok eltávolításra kerülhetnek, mindez nem vezethet azonban a demokratikus vita csorbításához, a plurális vélemények megismerésének ellehetetlenítéséhez.[647] Megemlítendő továbbá, hogy adott esetben akár a platformok által végzett értékelések, a platform által nyújtott ajánlások is tekinthetők véleménynek, az ezen tevékenység során nyert adatvagyonhoz pedig a platform-szolgáltatónak is fűződhetnek olyan érdekei, amelyek adott esetben alkotmányos védelemre tarthatnak számot.[648] Ennek tartalma és relevanciája azonban esetről-esetre, az adott adatkezelés sajátosságai, valamint az érintetti érdekek figyelembevételével vizsgálandó.

A fentiek mellett kiemelendő továbbá, hogy a DSA a kiskorúak magánéletét és személyes adatait védő rendelkezéseket is tartalmaz, így előírja, hogy a kiskorúak számára hozzáférhető online platformot üzemeltető szolgáltatók megfelelő intézkedéseket hozzanak a szolgáltatásukkal összefüggésben a kiskorúak magas szintű magánéleti védelme és biztonsága érdekében,[649] továbbá megtiltja a szolgáltatók számára profilalkotáson alapuló hirdetések megjelenítését, amennyiben a szolgáltató kellő bizonyossággal tudatában van annak, hogy a szolgáltatás igénybe vevője kiskorú.[650] Ennek körében kiemeli azonban, hogy a szolgáltató nem köteles annak értékelése érdekében további személyes adatok kezelésére, hogy az igénybe vevő kiskorú-e.[651] A fentiekre tekintettel a DSA több, a kiskorúak magánéletének, személyes adatai védelmével kapcsolatos követelményt is meghatároz, illetve – helyesen – tiltja a kiskorú felhasználók esetén profilalkotáson alapuló hirdetések megjelenítését, tekintettel arra, hogy ez a kiskorúak fejlődésére különösen káros lehet, illetve a felnőttekénél jóval nagyobb behatást eredményezhet jövőbeli magatartásukra, döntéseikre. Tekintettel azonban arra, hogy a

[645] DSA 27. cikk (2) bek.
[646] DSA 27. cikk (3) bek.
[647] TÖRÖK Bernát: Közösségi média – társadalmi párbeszéd. *Fundamentum*, 2022/3. 58–59.
[648] KOLTAY (2019) i.m. 205.
[649] DSA 28. cikk (1) bek.
[650] DSA 28. cikk (2) bek.
[651] DSA 28. cikk (3) bek.

szolgáltatók a felhasználók által, például a regisztrációkor megadott adatok alapján nem feltétlenül tudnak következtetni a felhasználók életkorára, így kérdéses, hogy a fenti követelmények hogyan érvényesülhetnek, ha a szolgáltató nem ellenőrzi megfelelően az online platformon regisztrálók életkorát.

Megemlítendő, hogy a DSA további személyes adatok védelmével, valamint átláthatóság biztosításával kapcsolatos követelményeket is meghatároz az ajánlórendszereket használó online óriásplatformot vagy nagyon népszerű online keresőprogramot üzemeltető szolgáltatók számára. Így az ilyen szolgáltatók kötelesek minden olyan ajánlórendszerünk esetén legalább egy olyan lehetőséget biztosítani, amely nem profilalkotáson alapul.[652] Emellett az online interfészükön hirdetéseket megjelenítő fenti szolgáltatóknak a hirdetésre vonatkozó információt tartalmazó adattárat is szükséges megjeleníteniük, az igénybe vevők hirdetésekkel kapcsolatos hatékony tájékoztatása érdekében.[653]

A fentiekre tekintettel a DSA új keretrendszert teremtett mind a szolgáltatók közötti versenynek, mind az ezek szolgáltatásait igénybe vevő felhasználóknak,[654] amelynek részét képezi a személyes adatok kezelésével kapcsolatos további szabályok bevezetése is, amely adott esetben kevesebb visszaélésre ad okot a személyes adatok kezelése, felhasználói tartalmak megjelenítése és felhasználása kapcsán. Megemlítendő ugyanakkor, hogy 2024 tavaszán az Európai Bizottság eljárást kezdeményezett a Meta-val szemben a DSA feltételezett megsértése miatt, a Meta hirdetési gyakorlata, valamint a közösségi média oldalain megjelenő politikai tartalmakkal, az álhírekkel és egyéb káros tartalmakkal szembeni fellépés hiányosságai okán.[655] Tekintve, hogy ez lesz az első jelentős ügy a DSA alatt, így egyelőre kérdéses, hogyan is zárul majd, illetve pontosan milyen irányt is vesz az eljárás.

Az adatgazdaság szabályozása vonatkozásában a DSA mellett részletes szabályokat fogalmaz meg a digitális piacokról szóló jogszabály („**DMA**”),[656] amely szintén bizonyos esetekben

[652] DSA 38. cikk
[653] DSA 39. cikk (1) bek.
[654] FIRNIKSZ Judit: Az interoperabilitásra vonatkozó elvárások a digitális piacok szabályozási kontextusában. *In Medias Res*, 2023/2. 121.
[655] European Commission, Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act, 30 April 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373
[656] Az Európai Parlament es a Tanács (EU) 2022/1925 rendelete, a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály), PE/17/2022/REV/1, HL L 265., 2022.10.12, p. 1–66 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

szintén jelentőséggel bír az MI-rendszerek platformokon végzett adatkezelései során. Tekintettel az értekezés adatvédelmi fókuszára, a DMA szabályainak részletes ismertetésétől azonban eltekintünk, és e tekintetben azon rendelkezéseket foglaljuk össze, amelyek a kapuőrök[657] tevékenysége vonatkozásában határoznak meg az MI általi adatkezeléssel kapcsolatos szabályokat. Ezen, jellemzően transzparenciával és a végfelhasználói adatok kezelésével kapcsolatos követelmények irányadók lehetnek akár az olyan MI megoldások (például: generatív MI megoldások) kapcsán is, amelyeket platformként nyújtanak.[658]

A fentiekre tekintettel a DMA megtiltja a kapuőrök számára online hirdetési szolgáltatások nyújtása céljából olyan végfelhasználók személyes adatainak kezelését, akik a kapuőr alapvető platformszolgáltatásait igénybe vevő harmadik felek szolgáltatásait veszik igénybe, illetve megtiltja a kapuőrök számára végfelhasználók beleptetését a kapuőr más szolgáltatásaiba személyes adatok összekapcsolása céljából.[659] A fenti tilalmak alól kivételt jelent azonban, ha a végfelhasználó számára a kapuőr konkrét választási lehetőséget kínált, amelyre tekintettel a végfelhasználó a fentiekhez hozzájárulást adott. A hozzájárulás megtagadása vagy visszavonása eseten azonban kapuőr egy éven belül nem ismételheti meg egynél többször a hozzájárulás iránti kérelmét ugyanarra a célra.[660] Emellett a kapuőr nem kényszerítheti az üzleti felhasználókat vagy végfelhasználókat további, illetve egyéb platformszolgaltatásai igénybevételére,[661] és így adott esetben további személyes adatok szolgáltatására.

A fentieken túl a kapuőröknek díjmentesen biztosítaniuk kell a végfelhasználók vagy az általuk felhatalmazott harmadik felek kérésére az alapvető platformszolgáltatás igénybevétele kapcsán általuk szolgáltatott vagy tevékenységük során keletkezett adataik tényleges hordozhatóságát.[662] Emellett a kapuőrnek az üzleti felhasználók es az általuk felhatalmazott harmadik felek részére is díjmentes hozzáférést kell biztosítania azon adatokhoz, amelyet ezen

[657] A DMA 3. cikkeben írtak szerint kapuőrnek minősített, alapvető platformszolgáltatásokat nyújtó vállalkozások (DMA 2. cikk 1. pontja). Megjegyzendő, hogy az Európai Bizottság számos jelentőség technológiai vállalatot jelölt ki kapuőrnek, illetve határozta meg az altaluk végzett alapvető platformszolgaltatásokat (ideértve például a Google keresőprogramot, a Facebook, az Instagram vagy a TikTok közösségi média oldalakat), lásd: European Commission, Gatekeepers, https://digital-markets-act.ec.europa.eu/gatekeepers_en.

[658] Ayse Gizem YASAR, Andrew CHONG, Evan DONG, Thomas Krendl GILBERT, Sarah HLADIKOVA, Roland MAIO, Carlos MOUGAN, Xudong SHEN, Shubham SINGH, Ana-Andreea STOICA, Savannah THAIS, Miri ZILKA: AI and the EU Digital Markets Act: Addressing the Risks of Bigness in Generative AI, arXiv:2308.02033, https://doi.org/10.48550/arXiv.2308.02033. 2.

[659] DMA 5. cikk (2) bek. a), d) pontja.

[660] DMA 5. cikk (2) bek.

[661] DMA 5. cikk (8) bek.

[662] DMA 6. cikk (9) bek.

üzleti felhasználók termékeivel és szolgáltatásaival kapcsolatba kerülő végfelhasználók a platformon keresztül adnak meg, illetve azon adatokhoz, amelyet az adott platform ezzel összefüggésben generál; személyes adatok eseten azonban csak akkor garantálható a hozzáférés ilyen üzleti felhasználók részére, amennyiben ahhoz az érintettek hozzájárultak.[663]

Kiemelendő továbbá, hogy a kapuőr nem hozhatja hátrányosabb helyzetbe a fenti jogaikkal elő üzleti felhasználókat vagy végfelhasználókat, es nem nehezítheti meg a végfelhasználók jogainak gyakorlását.[664] Kérdésesnek tekinthető azonban, hogy a DMA átláthatósággal kapcsolatos követelményei az online platformokra irányadó egyéb transzparencia-szabályok es a végfelhasználók jogait védő egyéb rendelkezések – a felhasználok által a gyakorlatban kevéssé olvasott általános szerződési feltételek, adatvédelmi tájékoztatok szövegének bővítésén kívül – mennyire biztosítanak majd valós védelmet az érintettek számára.[665]

Tekintettel az online platformokra és az adatvédelemre vonatkozó fenti követelményekre, valamint a jogsértő vagy félrevezető tartalmak meggátolásának, kiszűrésének fontosságára, az online platformok üzemeltetőinek jelentős része (ideértve például az ismertebb közösségi médiaszolgáltatókat) meghatározott már hirdetések megjelenésével, valamint a káros tartalmak kiszűrésével és jelentésével kapcsolatos szabályokat, az ezekről szóló, felhasználóknak címzett összefoglalók pedig jellemzően elérhetők az adott platformon keresztül. Így például a Facebook is lehetővé teszi a hírfolyamok testre szabását a felhasználók számára, hogy a felhasználók a számukra releváns híreket láthassák, a kapcsolódó beállítási lehetőségekről pedig tájékoztatást nyújt.[666]

Kiemelendő, hogy napjainkban a jelentősnek tekinthető online platformok (ideértve például az ismertebb közösségi médiaoldalakat), illetve a népszerű keresőszolgáltatások üzemeltetői aktívan használnak gépi tanulási megoldásokat a felhasználóknak szóló hirdetések megjelenítése kapcsán. Ennek kapcsán, különösen a közösségi médiaszolgáltatók esetén, jelentős szerepet játszik a személyiségprofilok létrehozása, különböző célcsoportok képzése, amelyek révén a szolgáltató azonosítani tudja a felhasználók érdeklődési körét, ennek, illetve a felhasználó korábbi magatartása, cselekvései, illetve a hasonló felhasználók érdeklődése

[663] DMA 6. cikk (10) bek
[664] DMA 13. cikk (6) bek
[665] ZŐDI (2022) 81–82.
[666] A Facebook-hírfolyamban megjelenő tartalmak beállítása, https://www.facebook.com/help/1913802218945435

alapján pedig a felhasználó részére nagyobb eséllyel tud az őt érdeklő tartalmakat ajánlani.[667] Így a Facebook például alapvetően az adott felhasználó hirdetési célcsoportba tartozása, valamint hirdetési aukciók eredménye alapján határoz a vonatkozó hirdetés megjelenítéséről, azonban ennek kapcsán jelentősége van egyéb körülményeknek, például a felhasználó magatartásának, illetve hirdetési beállításainak is. A felhasználó számára releváns tartalmak megállapítása kapcsán különös jelentősége van az MI alkalmazásának és a gépi tanulásnak, amelynek segítségével megjósolható például, hogy a felhasználót korábbi aktivitása (például: általa adott lájkok) tükrében mennyire érdekli majd az adott tartalom, illetve milyen eséllyel fog a hirdető által elvárt cselekvést végezni (például: a hirdetői honlapot felkeresni).[668] A Google keresési találataiban megjelenő hirdetések esetén is jelentősége van a hirdetésaukcióknak. Így amikor valaki keresést végez, a kulcsszavakkal egyezést mutató hirdetések közül szintén a kereső számára valószínűleg legrelevánsabbnak tekinthető keresési találatokat mutatja meg a Google, az ennek megfelelő sorrendben.[669]

Hangsúlyozandó, hogy a platformok alkalmazása kapcsán a közelmúltban jelentős vitát váltott ki a hozzájárulás vagy fizetési modell alkalmazása (például: a Facebook esetén), amely értelmében a felhasználók választhatnak, hogy vagy viselkedésalapú reklám céljára használja fel a platform személyes adataikat, vagy fizetnek a platform ezt nélkülöző alkalmazásáért. Az EDPB 2024. áprilisában több európai adatvédelmi hatóság megkeresését követően véleményt bocsátott ki ezen üzleti modell adatvédelmi megfeleléséről. Az EDPB véleményében kifejtette, miszerint a fenti modell nem teremt valós hozzájárulási lehetőséget az érintettek számára, így a platformoknak kínálniuk kell egy „megfelelő alternatívát", amely nem foglalja magában díj fizetését.[670] Amennyiben az adott szolgáltató megfelelő alternatívaként fizetős megoldást határoz meg, úgy javasolt díjfizetés nélküli további lehetőséget is felajánlani a felhasználók számára, amely esetén viselkedésalapú marketingre nem kerül sor, és a platform kevesebb személyes adatot használ fel reklámcélra, vagy ilyen adatkezelésre egyáltalán nem kerül sor (például: általános, személyre nem szabott reklámtartalmak, a felhasználó által választott érdeklődési kör(ök) szerinti tartalmak).[671] Kiemelendő, hogy amennyiben a platform

[667] KOLTAY András: A social media platformok jogi státusa a szólásszabadság szempontjából. *In Medias Res*, 2019/1. 25.
[668] Meta, Good Questions, Real Answers: How Does Facebook Use Machine Learning to Deliver Ads?, 2020.06.11, https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads
[669] Google Ads Súgó, Aukció, https://support.google.com/google-ads/answer/142918?hl=hu
[670] EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Adopted on 17 April 2024 ("**08/2024. sz. EDPB Vélemény**"). 73.
[671] 08/2024. sz. EDPB Vélemény, 74-75.

szolgáltatója díjfizetéses modellt is meghatároz, úgy e körben észszerű mértékű díjat kell meghatároznia, amely nem akadályozhatja az érintettet döntési szabadságának gyakorlásában, és összhangban áll a tisztességes adatkezelés elvével.[672] A fentiek értelmében tehát a platform felhasználói viselkedés elemzése, valamint reklámtartalmak megjelenítése kapcsán történő MI-alkalmazásának is meg kell felelnie a fenti követelményeknek, tiszteletben tartva a felhasználó döntési akaratát.

Hangsúlyozandó, hogy az egyes érintetti csoportokkal kapcsolatos – kezdetben statisztikai összesítéseken vagy egyéb nem személyes adatokon alapuló – adatkezelések már az adatvédelmi jogszabályok hatálya alá tartozhatnak, amennyiben a fejlesztés során személyes adatok a tanítóadatok részét képezik, míg a modell, illetve az azon alapuló MI-rendszer alkalmazása során olyan esetekben, amikor egy célcsoportra vonatkozó adatokat konkrét érintettre vonatkoztatják (például: egy felhasználó számára azért jelenít meg bizonyos tartalmakat vagy ajánlatokat a platform mert egy bizonyos korosztályba tartozik).[673] Megjegyzendő azonban, hogy a felhasználók maguk is jelentős felelősséggel rendelkeznek adataik megosztása kapcsán, illetve a tekintetben, hogy tevékenységük, magánéletük egyes részeit a nyilvánosság számára felfedik-e, az egyes róluk szóló tartalmakat, híreket megosztják-e egyes szolgáltatókkal vagy más felhasználókkal.[674] Ugyanakkor az internet széleskörű lehetőséget biztosít az anonim felhasználásra, véleménynyilvánításra (ideértve adott esetben a visszaélésszerű vagy mások számára sérelmes megnyilvánulásokat is),[675] továbbá a felhasználók közösségi média oldalak és számos egyéb weboldal vagy applikáció által lehetővé tett adatvédelmi beállítás révén szintén kinyilváníthatják adataik hozzáférhetőségével kapcsolatos döntésüket, így az online interakciók felelős szereplőiként eljárva.

5. A mesterséges intelligencia általi adatkezelés az Amerikai Egyesült Államokban

[672] 08/2024. sz. EDPB Vélemény, 132-135.
[673] ICO, How do we ensure lawfulness in AI?, What about inferences and affinity groups?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/
[674] BAKOS-KOVÁCS Kitti: Magánélet a hálózat csapdájában – a „személyiségprofilok" jogi értékelése. In: GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András (szerk.): *A személyiség védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017. 105.
[675] KOLTAY András: Az internetes kapuőrök mint szerkesztők – a kommentek kérdése. In: GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András (szerk.): *A személyiség védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017. 215.

Az MI-vel kapcsolatos szabályozási törekvések, valamint az európai technológiaszabályozás figyelemmel kísérése jelentős fejleményekhez vezettek az elmúlt években az Egyesült Államokban is. Az amerikai kormányzat felismerte ugyanis az MI gazdasági és társadalomformáló szerepét, és egyértelmű célul tűzte ki az MI területén az amerikai vezető szerep megszerzését, vagy épp megőrzését a világgazdaságban, amelyhez megfelelő szabályozási törekvést is rendelt. A szabályozáson túl azonban az amerikai bírói joggyakorlat is aktívnak mutatkozik, különösen a generatív MI megoldások, valamint a biometrikus MI-rendszerek alkalmazása, valamint az ezek révén végzett adatgyűjtés kapcsán.

Az alábbiakban az amerikai szövetségi, illetve tagállami MI szabályozást foglaljuk össze az MI általi adatkezelésre fókuszálva, valamint kiemeljük a bírósági gyakorlat egyes kulcsfontosságú szempontjait, ismertetjük az elmúlt időszak jelentősnek tekinthető döntéseit, illetve jogvitáit.

a. Az amerikai szabályozás

Az Egyesült Államok eltérő hagyományaira és történelmi tapasztalataira tekintettel az adatvédelem területén jelentősen más utat választott, mint az európai országok. Míg az EU a személyes adatok védelme területén átfogó adatvédelemi szabályozás kialakítását választotta, addig az amerikai modell alapvetően fogyasztóvédelmi megközelítés szerint alakult ki.[676] E tekintetben különösen a Kalifornia állam által 2018-ban elfogadott California Consumer Privacy Act („**CCPA**”)[677] jelentett fordulópontot, amely átfogó módon, a GDPR szabályait is alapul véve vezetett be fogyasztói adatok kezelésével kapcsolatos szabályozást. Ezt megelőzően sem szövetségi, sem tagállami szinten nem volt olyan jogszabály, amely az európai szabályozáshoz hasonlóan, átfogó adatvédelmi követelményeket támasztott volna.[678] Ezt megelőzően az amerikai szabályozás főként a *privacy* megközelítésre támaszkodott, amely elsősorban a magánélet, jóhírnév védelméből kiindulva igyekezett védelmet biztosítani az érintettek számára. Ennek lényeges összefoglalását elsőként Samuel D. Warren és Louis D. Brandeis későbbi legfelsőbb bírósági tagok adták „The Right to Privacy” című tanulmányukban, amelyben a *privacy* tárgyalása során különösen a magánélet védelmét

[676] William MCGEVERAN: Friending the Privacy Regulators. *Arizona Law Review*, vol. 58., issue 4. (2016). 965.
[677] California Consumer Privacy Act of 2018, https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law
[678] Anupam CHANDER, Margot E. KAMINSKI, William MCGEVERAN: Catalyzing Privacy Law. *Minnesota Law Review*, 105 (2021). 1738.

hangsúlyozták a technológiai fejlődés és a média térnyerése tükrében.[679] E körben szintén kiemeltnek tekintendő William R. Prosser kaliforniai professzor 1960-ban írt „Privacy" című tanulmánya, amelyben a „privacy" megsértésének eseteit foglalja össze, ideértve 1) a magánéletbe való beavatkozást, 2) az érintett számára megalázó privát információk nyilvánosságra hozatalát, 3) a hitelrontást, 4) valamint a név és megjelenés (*image*) kisajátítását.[680] Mindez napjainkra azonban megváltozott, és az amerikai adatvédelmi szabályozás többarcúvá vált – továbbra is jelentős szempontot képez a magánélet és a személyiségi jogok védelme, azonban európai mintára az adatvédelmi megközelítés is egyre nagyobb teret nyert, és egyre jelentősebb mértékben formálja az amerikai jogalkotást.[681]

A fentiekre tekintettel az Egyesült Államokban az MI általi adatkezelés jogszabályi kereteit különösen az irányadó szövetségi és tagállami adatvédelmi jogszabályi rendelkezések, valamint az adott területek, tevékenységek kapcsán elterjedt hatósági és szakmai iránymutatások, illetve a vonatkozói bírói gyakorlatban megjelenő elvárások, szempontok adják.

Szövetségi szinten az MI szabályozása szempontjából meghatározónak tekinthető a 2021-ben elfogadott National Artificial Intelligence Iniatiative Act.[682] Ezen jogszabály fogadja el a National Artificial Intelligence Initiative-et,[683] amely meghatározza az amerikai MI stratégia pillérjeit, ideértve például az innovációt vagy az egyes kiemelt szakterületeket, mint például az egészségügyet.[684] A fentieken túl értelemszerűen a különböző adatvédelmi jogszabályok jellemzően az MI általi adatkezelésekre is kiterjednek, ideértve például az egészségügyi vagy a banki, illetve a pénzügyi szolgáltatók általi adatkezelésre vonatkozó jogszabályi rendelkezéseket. Emellett a fentebb írtak szerint az algoritmusok általi diszkriminációval szembeni küzdelem is jelentős szabályozási célnak tekinthető, amely tükrében a kialakulóban lévő szabályozás vélhetőleg más országok számára is meghatározó lesz majd.

---

[679] Samuel D. WARREN – Louis D. BRANDEIS: The Right to Privacy. *Harvard Law Review*, vol. 4., no. 5. (1890) 196.
[680] William L. PROSSER: Privacy. *California Law Review*, vol. 48., no. 3. (1960) 389.
[681] Az európai és amerikai adatvédelmi jog történeti szempontjai, összevetése kapcsán lásd továbbá: Daniel NECZ: Data Segregation and its Privacy Aspects. *Iustum Aequum Salutare*, XIX/2023. 3. 248–249.
[682] National Artificial Intelligence Initiative Act of 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210
[683] National Artificial Intelligence Initiative, https://www.ai.gov/
[684] NECZ (2022b). i. m. 113.

A fentiek mellett megemlítendő, hogy 2023-ban benyújtásra került az „AI Foundational Model Transparency Act" elnevezésű törvény-tervezet,[685] amely a generikus MI-modellek kapcsán támaszt átláthatósággal kapcsolatos követelményeket. A törvény-tervezet az olyan vállalkozásokra vonatkozik, amelyek olyan modellre támaszkodnak, illetve használnak szolgáltatásaik kapcsán, amely átlagosan havonta több mint 100.000 eredményt („*output instances*") generál (ideértve például szöveges, képi, videó, hanganyag vagy egyéb eredmény) vagy átlagosan havonta több mint 30.000 felhasználóval rendelkezik.[686] A jogszabály értelmében továbbá ezen szolgáltatóknak nyilvánosságra kellene hozniuk a modell fejlesztéséhez felhasznált tréningadatok forrásait és egyéb lényegi jellemzőit, valamint a modellel kapcsolatos kockázatokat és egyéb lényeges információkat.[687]

Az MI általi adatkezelés szabályozásával kapcsolatban azonban kifejezetten a tagállami szabályozás mondható jelentősnek. Az MI általi adatkezelésre vonatkozóan ennek kapcsán a tagállami jogszabályok több szempontból is az európai szabályozáshoz hasonló rendelkezéseket tartalmaznak. Így például a kaliforniai szabályozás is a GDPR-hoz hasonlóan határozza meg az automatizált döntéshozatal fogalmát,[688] emellett szintén a GDPR-hoz hasonlóan határozza meg az automatizált döntéshozatallal járó technológiával, illetve profilalkotással kapcsolatos adatkezeléssel szemben való tiltakozáshoz való jogot, valamint az alkalmazott logikára, fogyasztóra kiható eredményekre vonatkozó információhoz való hozzáférésre vonatkozó jogot.[689] Így azonban az automatizált döntéshozatal kapcsán az európai szabályozáshoz hasonlóan a kaliforniai szabályozás is a személyes adatok kezelésére és azok védelmére helyezi a hangsúlyt az érintettekre gyakorolt hatások megfelelő mértékű figyelembevétele helyett.[690]

[685] AI Foundation Model Transparency Act of 2023, https://beyer.house.gov/uploadedfiles/ai_foundation_model_transparency_act_text_118.pdf
[686] AI Foundation Model Transparency Act, sec. 3(3)(A)
[687] AI Foundation Model Transparency Act, sec. 3(f)
[688] CCPA 1798.140(z)
[689] CCPA 1798.185(16). Az egyes tagállami szabályozásokkal kapcsolatban lásd továbbá: Necz (2022b). i. m. 114–115.
[690] Eli MACKINNON, Dr. Jennifer KING: Regulating AI Through Data Privacy. Stanford University. *Ethics and Justice, Law, Regulation, and Policy*, 2022.01.11, https://hai.stanford.edu/news/regulating-ai-through-data-privacy

Jelentős fejleményt jelent a szövetségi szabályozás kapcsán az American Privacy Rights Act („**APRA**”) elnevezésű törvény-tervezet,[691] amely átfogó, egységes szabályozási keretrendszert nyújtana az amerikai adatvédelem és adatbiztonság területén, figyelembe véve az európai és a tagállami jogfejlődés irányait is. Az APRA így a tagállami adatvédelmi szabályozást is számos esetben hatályon kívül helyezné,[692] így egységesítve a jelenleg széttagoltnak tekinthető, sok esetben tagállami hangsúlyt élvező amerikai adatvédelmi szabályozást. Az APRA kiterjed egyrészt a szabályozott szervezetekre („*covered entity*”), másrészt a szolgáltatókra („*service provider*”). Az APRA a szabályozott szervezetek körébe érti – a GDPR mintájára – a szabályozott adatkör kezelése céljait és eszközeit meghatározó szervezeteket, amelyek felügyelete az FTC hatáskörébe tartozik, illetve amelyek szállítást végző vállalkozásnak („*common carrier*”) vagy non-profit szervezetnek minősülnek,[693] míg szolgáltatónak tekinti azon szervezeteket, amelyek a szabályozott szervezet nevében és irányítása alapján járnak el.[694] Hangsúlyozandó, hogy az APRA meghatározza azon adatkört is, amelyre a jogszabály hatálya kiterjed, ideértve azon információkat, amelyek önmagukban vagy más információkkal együttesen egy érintettet azonosítanak, illetve az érintetthez kapcsolódnak vagy észszerűen hozzá kapcsolhatók, illetve kiterjed az olyan információkra is, amelyek egy vagy több érintettet azonosítanak, illetve hozzá vagy hozzájuk kapcsolódnak vagy észszerűen hozzá kapcsolhatók.[695]

Az APRA az európai adatvédelmi szabályozás mentén számos kötelezettséget rögzít a fenti szervezetekre, ideértve az adatminimalizálás követelményét,[696] az átláthatósághoz való jogot,[697] az érintett rendelkezési jogát az adatok felett,[698] valamint az érintett tiltakozáshoz való jogát egyes adattovábbítások,[699] és a direkt marketing tevékenység esetén.[700] Az APRA továbbá többlet-követelményeket határoz meg a jelentős hatással bíró közösségi média társaságokra („*high-impact social media company*”), valamint a jelentős adatbirtokosokra („*large data holder*”) nézve. Az APRA az előbbi körbe érti azon szabályozott szervezeteket, amelyek a)

[691] American Privacy Rights Act of 2024, https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf
[692] ARPA, Sec. 20(a).
[693] ARPA, Sec. 2(10).
[694] ARPA, Sec. 2(35).
[695] ARPA, Sec. 2(9).
[696] ARPA, Sec. 3.
[697] ARPA, Sec. 4.
[698] ARPA, Sec. 5.
[699] ARPA, Sec. 6(1).
[700] ARPA, Sec. 6(2).

legalább 3 milliárd dollár éves világbevétellel rendelkeznek, b) világszinten legalább 300 millió felhasználóval rendelkeznek legalább 3 hónapon át a megelőző 12 hónapon belül, valamint c) a főként felhasználók által készített tartalmak elérésére, megosztására szolgáló platformokat,[701] míg az utóbbi körbe azon szabályozott szervezeteket vagy szolgáltatókat érti, amelyek legalább 250 millió dollár bruttó világbevétellel rendelkeztek a megelőző üzleti év során, és amelyek meghatározott számú érintettre, hordozható eszközre, illetve eszközre vonatkozó szabályozott adatot vagy szenzitív szabályozott adatot gyűjtöttek, dolgoztak fel, birtokoltak vagy továbbítottak.[702]

Az APRA külön szabályokat határoz meg a szabályozott algoritmusok alkalmazóira. Ezen algoritmusok szabályozott adatokra támaszkodva végeznek automatizált döntéshozatalt, vagy támogatják az emberi döntéshozatalt.[703] Az APRA szabályainak tükrében már a szabályozott algoritmusok tervezése során törekedni kell a károk elkerülésére, és esetleges felmérésére,[704] emellett az ilyen algoritmust alkalmazó jelentős adatbirtokosoknak hatásvizsgálatot szükséges végezniük.[705] Emellett az APRA az egyes jelentős döntések (például: egyes alapvető szolgáltatások nyújtása) meghozatala céljából alkalmazott algoritmusok által érintettetek figyelmeztetését is előírja az ilyen algoritmusok alkalmazására, valamint tiltakozási jogot biztosít az érintettek számára.[706] Mindezen szabály elejét venné például, hogy az olyan jelentős döntéseket, mint az érintett egyetemi felvétele, az algoritmus hozzon meg az érintettek számára átláthatatlan módon.

A fentiekre tekintettel az amerikai szabályozás jelentős hangsúlyt fektet az automatizált döntéshozatal, valamint a profilalkotás szabályozására, továbbá az európai szabályozás vívmányait egyre fokozott mértékben veszi át. Emellett azonban számos egyéb szempontot is érvényre juttat e téren, ideértve különösen – a korábban jellemzően állampolgári jogokban, egyes területeken, például: pénzügyi szolgáltatások, lakhatás kapcsán megjelenített[707] – diszkrimináció elleni küzdelmet, valamint az adatkezelést végzők és a kezelt adatok körének kockázatalapú szabályozását. E tekintetben különösen a tagállami szabályozás tekinthető

[701] ARPA, Sec. 2(11).
[702] ARPA, Sec. 2(25).
[703] ARPA, Sec. 2(8).
[704] ARPA, Sec. 13(c)(2).
[705] ARPA, Sec. 13(c)(1).
[706] ARPA, Sec. 14.
[707] Kirk J. NAHRA: The Past, Present, and Future of U.S. Privacy Law. *Seton Hall Law Review*, vol. 51., issue 5 (2021) 1562.

dinamikusnak, azonban az egyes szabályok többször az európai szabályozás szövegét veszik alapul és próbálják amerikai viszonyok közé adaptálni. Ezen megközelítés azonban a közeljövőben jelentősen változhat, tekintettel az APRA keretrendszer jellegére.

b. Az amerikai bírósági gyakorlat

Az amerikai technológiai szektor az MI területén jelentős eredményeket ért el az utóbbi időben. Ennek kapcsán elengedő, ha csak a legismertebb MI-modellek, mint például a GPT, elterjedésére, vagy az MI-re fókuszáló vállalatok, szervezetek, mint például az OpenAI, a Mircosoft vagy a Google eredményeire gondolunk. Napjainkban a technológiai nagyvállalatok jellemzően már jelentős hangsúlyt helyeznek az adatvédelmi követelményeknek való megfelelésre, és ezt igyekeznek üzletpolitikájukban is megjeleníteni.[708] Mindazonáltal az MI megoldások értelemszerűen jelentős adatéhséggel bírnak, a korábbi fejezetekben ismertetettek szerint pedig ezen megoldások alkalmazása a nagyvállalatok birtokában lévő beláthatatlan adattömegeken sokszor feszegeti az adatvédelem követelményeit és határait.

A fentiekre tekintettel az utóbbi időben az amerikai bírói gyakorlatban az MI megoldások alkalmazásával kapcsolatos jogviták is megszaporodtak. 2023. júliusában például a Google-el szemben indítottak csoportos pert (angolul: „*class action*") Kaliforniában, arra hivatkozással, hogy a Google MI fejlesztése során közösségi média oldalakon és egyéb weboldalakon elérhető tartalmakat és adatokat használ fel jogsértő módon, így az érintettek személyiségi jogait és szellemi tulajdonjogát is sértve.[709] Hasonlóan – többek között – adatvédelmi jogsértés miatt indult per az elmúlt időszakban több más technológiai vállalat, köztük a ChatGPT megoldást fejlesztő és biztosító OpenAI vállalat ellen is.[710]

További főbb csoportnak tekinthetők a biometrikus adatkezeléssel foglalkozó vállalatok elleni perek. Így például az arcképelemzéssel kapcsolatos szolgáltatásokat biztosító vállalat, a Clearview AI elleni per egyezséggel zárult 2022. májusában. A pert az ALCU, valamint számos más amerikai civil szervezet kezdeményezte, tekintettel arra, hogy álláspontjuk szerint a Clearview AI arcképgyűjtéssel és elemzéssel, valamint kapcsolódó szolgáltatások nyújtásával kapcsolatos gyakorlata sérti az érintettek adatvédelmi jogait, valamint a biometrikus adatok

[708] MCGEVERAN i.m. 986.
[709] L. v. Alphabet Inc. Alphabet Inc., 3:23-cv-03440 (N.D. Cal. 2023) [71]–[97]
[710] P.M. v. OpenAI LP, 3:23-cv-03199 (N.D. Cal. 2023) [264]–[274]

kezelésével kapcsolatos vonatkozó jogszabályi rendelkezéseket. Az egyezség révén a Clearview AI adatbázisából törölhetik magukat az érintettek Illinois tagállamban, a társaság pedig nem értékesítheti arcképadatbázisát üzleti vállalkozások és magánszervezetek részére, továbbá öt évig Illinois államban sem végezhet ilyen értékesítési tevékenységet a tagállami és helyi rendőrhatóságok részére.[711] A Vimeo nevű videómegosztó-platform szolgáltatójával szembeni per[712] ugyancsak egyezséggel zárult, amelyben a Vimeo több mint 2 millió dolláros kártérítés megfizetését vállalta a platformájára feltöltött videótartalmakkal kapcsolatos jogsértő arcfelismerő technológia alkalmazására tekintettel.[713] Emellett az FTC is 2023. decemberében nyújtott be keresetet a Rite Aid Corporation nevű szervezettel szemben arcfelismerő rendszer alkalmazásával kapcsolatban, illetve annak okán, hogy a szervezet a technológia alkalmazása során nem tartotta be a diszkriminációtilalommal kapcsolatos jogszabályi rendelkezéseket.[714]

Említésre érdemes továbbá a New York Times nevű ismert amerikai lap OpenAI ellen kezdeményezett keresete is. Habar az ügy alapvetően szerzői jogi természetű, és a szerzői jog által védett művek jogsértő bányászatára es felhasználására fókuszál, adatvédelmi tárgyú relevanciával is bír. A New York Times a lap weboldalan ún. fizető fal (angolul: „*paywall*") megoldást alkalmaz, aminek lényege, hogy bizonyos tartalmakat vagy azok jelentős részét csak az előfizetők számára jeleníti meg, míg az oldal egyéb látogatói azokhoz előfizetés hiányában nem férhetnek hozza. A kereset tanúsága szerint azonban a OpenAI által fejlesztett ChatGPT alkalmazás a felhasználók számára mégis megjelenített számos olyan cikket amelyek csak előfizetés útján lennének elérhetők az olvasok számára.[715] Érdekes kérdésnek tekinthető, hogy vajon hasonló MI megoldások személyes adatokhoz is hozzáférnek-e zártan kezelt vagy utóbb korlátozott elérhetőséggel bíró oldalakhoz, adatbázisokhoz (például: felhasználói profilok, amelyek nyilvános elérhetőséget később korlátoztak), és ha igen, azokat milyen mértékben használjak azokat fel. E tekintetben álláspontunk szerint ki kell alakulnia egy egyértelmű es következetes gyakorlatnak, amelyet mind a piaci szereplők nagyrésze, mind az adatvédelmi hatóságok es bíróságok követendőnek tartanak.

[711] John v. Clearview AI, Inc., 1:20-cv-03481 (District Court, S.D. New York, 2020) [66]–[86]
[712] Acaley v. Vimeo, Inc., 464 F. Supp. 3d 959, 969 (N.D. Ill. 2020)
[713] IAPP. Vimeo settles biometric privacy lawsuit; Tesla faces privacy class action, 2023.04.11, https://iapp.org/news/a/vimeo-settles-biometric-privacy-lawsuit-tesla-faces-privacy-class-action/
[714] Fed. Trade Comm'n v. Rite Aid Corp., 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023) [50]–[84]
[715] The New York Times Company v. Microsoft Corporation, 1:23-cv-11195 (District Court, S.D. New York, 2023) [32]–[37]

Ahogy az a fentiekből is látszik, az Egyesült Államokban az MI általi adatkezelések kapcsán különösen az egyes MI-modellek szolgáltatói általi adatgyűjtéssel, valamint az arcfelismerő technológia alkalmazásával kapcsolatos jogviták mondhatók jelentősnek. Habár a vonatkozó peres eljárások egy része még folyamatban van, illetve az irányadó szabályozás napjainkban még alakulóban lévőnek tekinthetők, a fenti jogviták jól jelzik az átlátható és megfelelő jogalapokon nyugvó adatkezelés fontosságát, továbbá az érintetti jogok támogatásának szükségességét.

6. A mesterséges intelligenciával kapcsolatos különös adatvédelmi kihívások

A digitalizáció és az MI adta forradalmi változások jelentős kihívások elé állítják a szabályozókat világszerte. Természetesen az új technológiák szabályozása nem vezethet a technológiai fejlődés aránytalan korlátozásához, azonban az érintettek és a társadalom számára kiemelt kockázattal bíró megoldások kapcsán megfelelő követelmények előírása lehet indokolt.

A fentebb írtakra is tekintettel az alábbi sorokban főként azon újabb technológiai megoldásokra fókuszálunk, amelyek álláspontunk szerint különös társadalomformáló erővel bírhatnak a közeljövőben, és amelyekre napjaink adatvédelmi szabályozása, különösen az EU-n belül, általában nehézkesen képes reagálni. Ezek között tárgyaljuk az általános célú MI általi adatkezeléssel kapcsolatos szabályozást és problémákat, valamint a közbeszédre is jelentős formálóerővel bíró deepfake technológiát és a demokratikus társadalmak szempontjából ugyancsak jelentős hangsúllyal bíró arcfelismerő rendszereket, amelyek alapjaiban határozzák meg az egyén és a kormányzat viszonyát, valamint az egyén szabadságának kereteit.

a. Az általános célú mesterséges intelligencia

Az általános célú MI forradalminak tekinthető hatásai napjainkban szintén számos területen megmutatkoznak, tekintettel ezen megoldások multimodális jellegére. Az ilyen modellek fejlesztéséhez jellemzően nyilvános forrásból (ideértve különösen a publikus internetet) kerül sor nagyméretű információ összegyűjtésére és elemzésére, jellemzően komplex műveletek eredményeként. Mindez értelemszerűen szembe megy a GDPR-ban is megjelenő adatvédelmi alapelvekkel, és az érintettek számára sokszor átláthatatlan adatkezelések sorozatához vezet, különös tekintettel az általános célú MI-modellek sokoldalú felhasználására.

Habár az általános célú MI sokáig nem rendelkezett, illetve sok esetben a gyakorlatban mai napig nem rendelkezik általános és egységesen alkalmazandó fogalom-meghatározással,[716] az MI Rendelet erre mégis kísérletet tesz. Az MI Rendelet az általános célú MI-modellt akként határozza meg, mint „*olyan MI-modell – ideértve azt is, amikor az ilyen MI-modell tanítása nagy adatmennyiséggel, nagy léptékű önfelügyelet mellett történik –, amely jelentős általánosságot mutat, és forgalomba hozatalának módjától függetlenül, különféle feladatok széles körének elvégzésére képes, valamint többféle downstream rendszerbe vagy alkalmazásba integrálható, azon MI-modellek kivételével, amelyeket a forgalomba hozatalukat megelőzően kutatási, fejlesztési vagy prototípus-alkotási tevékenységekre használnak*”.[717] Az általános célú MI-modellektől megkülönböztetendők az általános célú MI-rendszerek,[718] amelyek általános célú modelleken alapulnak, és alkalmazhatók önállóan vagy más rendszerekbe integráltan is. Így például általános célú MI-modellnek tekintendő a GPT-modell, míg azon alapuló rendszernek a népszerű ChatGPT chatbot alkalmazás.[719]

Az MI-modellekre eltérő szabályok vonatkoznak, mint a modelleken alapuló MI-rendszerekre. Tekintettel azonban az általános célú MI-modellek jelentőségére, illetve arra a tényre, hogy számos rendszer alapjául szolgálnak, így ezek kapcsán az MI Rendelet is sajátos követelményeket határoz meg. Az MI Rendelet értelmében az általános célú MI-modellek szolgáltatói kötelesek

- az adott modellel kapcsolatos műszaki dokumentáció elkészítésére és napra készen tartására, amely kitér a modell tanítási és tesztelési folyamatára, valamint az értékelésének eredményeire;
- az adott modellel kapcsolatos megfelelő dokumentáció és információk kidolgozására és napra készen tartására, a modellt saját rendszereikbe beépíteni kívánó szolgáltatók számára. Ezen információknak és dokumentációnak lehetővé kell tenniük a modell képességeinek és korlátainak megértését, valamint, hogy ezen szolgáltatók ennek kapcsán az MI Rendelet szerinti saját kötelezettségeiknek is meg tudjanak felelni;

[716] Carlos I. GUTIERREZ, Anthony AGUIRRE, Risto UUK, Claire C. BOINE, Matija FRANKLIN: A Proposal for a Definition of General Purpose Artificial Intelligence Systems. *Digital Society*, 2/36. (2023) 3.
[717] MI Rendelet 3. cikk 63. pontja
[718] „*Általános célú MI-modellen alapuló MI-rendszer, amely – mind közvetlen felhasználás, mind más MI-rendszerekbe való integráció céljából – többféle célt képes szolgálni*” (MI Rendelet 3. cikk 66. pontja).
[719] ZŐDI Zsolt: A generatív mesterséges intelligencia szabályozása az MI rendeletben, 2024.04.29, https://www.ludovika.hu/blogok/itkiblog/2024/04/29/a-generativ-mesterseges-intelligencia-szabalyozasa-az-mi-rendeletben/

- a vonatkozó uniós jognak való megfelelésre irányuló politikát kell bevezetniük;
- kellő részletességű összefoglalót kell készíteniük és közzétenniük az általános célú MI-modell tanításához használt tartalomról,[720] ideértve különösen a modell tanítására felhasznált fő adatgyűjtemények vagy -készletek (például a nagy magán- vagy nyilvános adatbázisok, adatarchívumok) felsorolását, valamint az egyéb felhasznált adatforrások részletes leírását.[721]

A fentiek kapcsán megemlítendő azonban, hogy az általános célú MI-modellek szolgáltatóira vonatkozó kötelezettségek attól függetlenül irányadók, hogy az adott modell hogyan kerül forgalmazásra, azonban az MI Rendelet nem vonatkozik az olyan modellekre, amelyeket a forgalmazásuk előtt kutatási, fejlesztési célra, illetve prototípusként használnak.[722] Hangsúlyozandó, hogy a fenti első két kötelezettség nem vonatkozik az olyan MI-modellek szolgáltatóira, „*amelyeket olyan szabad és nyílt forráskódú licenc alapján bocsátanak ki, amely lehetővé teszi a modellhez való hozzáférést, annak használatát, módosítását és terjesztését, és amelyek paramétereit – beleértve a súlyokat, a modell-architektúrára vonatkozó információkat és a modellhasználatra vonatkozó információkat – nyilvánosan hozzáférhetővé teszik*”.[723] A gyakorlatban ilyennek minősülhetnek például az ismertebb TensorFlow vagy PyTorch keretrendszer vagy a képfeldolgozás területén jelentősnek mondható OpenCV,[724] illetve a 2023-ban alakult, nyílt forráskódú LLM rendszerek fejlesztésével foglalkozó Mistral AI elnevezésű francia vállalat megoldásai.[725]

A fentieken túl a rendszerszintű kockázatot jelentő általános célú MI-modellek szolgáltatóira további kötelezettségek vonatkoznak az MI Rendelet alapján. Az adott MI-modell abban az esetben tekintendő rendszerszintű kockázatot jelentőnek, amennyiben

- megfelelő technikai eszközök és módszertanok – többek között mutatók és referenciaértékek – alapján értékelt, nagy hatású képességekkel rendelkezik; vagy
- a Bizottság határozata alapján az adott modell a fentebb meghatározottakkal egyenértékű képességekkel vagy hatással rendelkezik.[726]

[720] MI Rendelet 53. cikk (1) bek.
[721] MI Rendelet (107) preambulum-bekezdés
[722] MI Rendelet 3. cikk 63. pontja
[723] MI Rendelet 53. cikk (2) bek.
[724] Tim MUCCI: Five open-source AI tools to know, 2023.12.15, https://www.ibm.com/blog/five-open-source-ai-tools-to-know/
[725] Mistral AI, https://mistral.ai/
[726] MI Rendelet 51. cikk (1) bek.

Az MI Rendelet vélelme alapján megállapítható, hogy az adott általános célú MI-modell nagy hatású képességekkel bír, amennyiben amikor a tanításához használt, lebegőpontos műveletekben mért, összesített számítási összege nagyobb, mint 10^25,[727] amely mérőszám szükség szerinti módosítása érdekében a Bizottság felhatalmazáson alapuló jogi aktusokat fogadhat el, valamint szükség esetén kiegészítheti a vonatkozó referenciamutatókat és a referenciaértékeket abból a célból, hogy ezen küszöbértékek a technika mindenkori állását tükrözzék.[728] Hangsúlyozandó, hogy a fenti, rendszerszintű kockázatot jelentő MI-modellek szolgáltatói kötelesek a fenti követelmény teljesülése esetén, de legfeljebb 2 héten belül értesíteni a Bizottságot az erre vonatkozó információk szolgáltatásával. Kiemelendő, hogy amennyiben a Bizottság nem kerül értesítésre arról, hogy az adott MI-modell rendszerszintű kockázatot jelentő MI modellnek minősül, azonban arról a Bizottság tudomást szerez, úgy szintén dönthet az adott modell rendszerszintű kockázatot jelentő modellé történő minősítéséről.[729] Ennek értelmében tehát a szolgáltatók az értesítés elmulasztásával önmagában nem kerülhetik el a modell rendszerszintű kockázatot jelentő modellé történő minősítését. A szolgáltató azonban az értesítésében hivatkozhat arra, hogy az adott modell annak sajátos jellemzői miatt rendszerszintű kockázatot nem jelent, [730] amelyet adott esetben a Bizottság figyelembe vesz, vagy elutasít, és az adott modellt rendszerszintű kockázatot jelentő MI-modellnek tekinti.[731]

Megemlítendő, hogy a rendszerszintű kockázatot jelentő általános célú MI-modellek szolgáltatói megfelelően alátámasztott ezirányú kérelmük esetén később is kérhetik a minősítés újraértékelését, azonban erre legkorábban a minősítéstől, illetve ennek Bizottság általi későbbi megerősítése esetén az ezt követő 6 hónapon belül kerülhet sor.[732] Emellett a rendszerszintű kockázatot jelentő MI-modellek listáját a Bizottság nyilvánosságra hozza,[733] így az adott modell rendszerszintű kockázatairól a nyilvánosság is tudomást szerezhet.

[727] MI Rendelet 51. cikk (2) bek.
[728] MI Rendelet 52. cikk (3) bek.
[729] MI Rendelet 52. cikk (4) bek.
[730] MI Rendelet 52. cikk (2) bek.
[731] MI Rendelet 52. cikk (3) bek.
[732] MI Rendelet 52. cikk (5) bek.
[733] MI Rendelet 52. cikk (6) bek.

A fentiekre tekintettel a rendszerszintű kockázatot jelentő általános célú MI-modellek szolgáltatói – a további általános céli MI-modellre irányadó követelmények teljesítésén túl – kötelesek

- modellértékelést végezni a technika állásának megfelelő, szabványosított protokollokkal és eszközökkel összhangban;
- értékelni és enyhíteni az esetlegesen a rendszerszintű kockázatot jelentő általános célú MI-modellek fejlesztéséből, forgalomba hozatalából vagy használatából eredő lehetséges, uniós szintű rendszerszintű kockázatokat;
- nyomon követni, dokumentálni és indokolatlan késedelem nélkül jelenteni az MI-hivatal és adott esetben az illetékes nemzeti hatóságok részére a súlyos váratlan eseményekre és az azok kezelésére szolgáló lehetséges korrekciós intézkedésekre vonatkozó releváns információkat;
- megfelelő szintű kiberbiztonsági védelmet biztosítani az MI-modell és a modell fizikai infrastruktúrája számára.[734]

A fentiekkel összhangban megállapítható továbbá, hogy az általános célú MI-modellek szolgáltatói számára értékes és hasznos adatnak tekinthetők az egyes nyilvános vagy egyéb forrásokból elért információkon túl adott esetben a felhasználók által megadott információk is, ideértve például a felhasználók által adott utasításokat (prompt) vagy a felhasználók által feltöltött tartalmakat (például: fényképek, videók, hanganyagok). Ebbe adott esetben beletartozhatnak a gyakorlatban kérdésesen felhasználható tartalmak, például magánszemélyeket vagy rendvédelmi szervek dolgozóit ábrázoló, főként olyan felvételek, amelyek nyilvános eseményeket jelenítenek meg vagy közterületen készültek, így nehéz lenne róluk kihagyni ezen felismerhető személyeket.[735] A ChatGPT-t szolgáltató OpenAI például a felhasználók által a chatablakban megadott információkat alapértelmezetten felhasználja a ChatGPT modelljének fejlesztéséhez, azonban ezzel szemben a felhasználók a felületen tiltakozhatnak (opt-out).[736] A Midjourney nevű, főként gépgenerálás céljára szolgáló megoldás szolgáltatója adatvédelmi tájékoztatójában már jellemzően csak általánosságban fogalmaz, így e tekintetben kérdésesnek tekinthető, hogy a felhasználói adatokat pontosan milyen célokra

[734] MI Rendelet 55. cikk (1) bek.
[735] PAPP János Tamás: A rendőrök képmáshoz való jogának kérdése. In: GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András: *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017. 122.
[736] OpenAI, How your data is used to improve model performance, https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance

használják fel, és az esetleges felhasználási módokkal szemben az érintettek milyen jogokkal bírnak.[737] A Google Gemini nevű multimodális MI-modellje kapcsán szintén számos adatot gyűjt a felhasználóktól, ideértve a Gemini-vel folytatott „beszélgetéseket", lokációs adatokat, felhasználói visszajelzéseket, használattal kapcsolatos információkat. A felhasználóknak a Gemini esetén is lehetőségük van a vonatkozó felületen meggátolni, hogy a Google generatív gépi tanulási technológiái fejlesztéséhez használja fel a felhasználók adatait (ide nem értve az adott „beszélgetések" kapcsán benyújtott felhasználói visszajelzéseket).[738]

A fentiek értelmében tehát megállapítható, hogy a legjelentősebbnek mondható multimodális MI-modellek szolgáltatói sok esetben törekednek a felhasználók számára is egyértelművé tenni jogaikat, valamint lehetővé tenni számukra, hogy felhasználói beállítások révén tiltakozzanak az adataik MI fejlesztés érdekében történő felhasználása ellen. Az olyan alapvető adatvédelmi követelmények, mint az adatminimalizálásnak vagy az adatkezelés pontos céljának meghatározása azonban különösen az általános célú MI-modellek esetén tűnnek teljesíthetetlennek.[739] Emellett az általános célú modellek (és a hozzájuk kapcsolódó adatkészletek) alapulvételével, felhasználásával végzett adatkezelések átláthatósága több szempontból így is kérdésesnek tekinthető, az érintettek jogai nehézkesen biztosíthatók az adatvédelmi jogszabályok, különösen a GDPR által megkövetelt mértékben és módon.

b. A deepfake technológia adatvédelmi kihívásai

Az elmúlt években különösen jelentős kihívássá vált az ún. deepfake tartalmakra való reagálás, valamint ezek szabályozása. Deepfake alatt jellemzően olyan szintetikus képi, hang, illetve videótartalmakat értünk, amelyek valótlanul másokat személyesítenek meg; a „deepfake" kifejezés pedig ennek kapcsán 2017 végén terjedt el az interneten, és első körben olyan felvételekre használták, amelyeken ismert emberek arcképe jelent meg pornográf tartalmakba ágyazottan.[740] A deepfake tartalmak azonban napjainkra egyéb területeken is elterjedtté váltak. Továbbra is számos esetben használják például a technológiát közszereplők kifigurázása vagy

[737] Midjourney, Privacy Policy, https://docs.midjourney.com/docs/privacy-policy, 2. és 6. pontok
[738] Google. Gemini Apps Privacy Hub, https://support.google.com/gemini/answer/13594961?hl=en#collected_data&zippy=%2Cwhy-does-google-retain-my-conversations-after-i-turn-off-gemini-apps-activity-and-what-does-google-do-with-this-data. Lásd különösen: „*What data is collected? How is it used?*", „*Why does Google retain my conversations after I turn off Gemini Apps Activity and what does Google do with this data?*"
[739] WOLFF, LEHR, YOO op. cit. 17.
[740] Meredith SOMERS: Deepfakes, explained, *MIT Management Sloan School*, 2020.07.21, https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

kritizálása céljából (például: a politikai humor eszközeként vagy szatirikus tartalmak elkészítéséhez), azonban egyre gyakrabban használják reklámcélból vagy bizonyos szolgáltatások nyújtása kapcsán is.

Sajnálatos módon azonban a különböző jogsértő felhasználások is megszaporodtak, illetve sokrétűvé váltak az elmúlt években. Napjainkra ugyanis már nem pusztán a hírességek válhatnak célponttá. A deepfake technológiát alkalmazó bűnözők politikusokat, szakértőket, cégvezetőket, vagy akár más személyeket is célba vehetnek, akiktől pénzt vagy egyéb ellenszolgáltatást remélhetnek, illetve akiket valamely okból kompromittálni akarnak. Sok esetben a csalók például bankokat keresnek meg az ügyfeleik hangját imitálva, annak reményében, hogy pénzügyi tranzakciók végzését érjék el.[741] A deepfake továbbá az egyes eljárások, jogviták során alkalmazott bizonyítékokra is hatással lehet, hiszen a deepfake technológiára való hivatkozás, adott esetben megkérdőjelezheti például egy hangfelvétel vagy egy kamerafelvétel eredetiségét, amelyet ilyen esetben az eljárás során majd szintén ellenőrizni, adott esetben bizonyítani kell.[742] Mindemellett a deepfake technológia az elmúlt években a személyiséglopások mellett az álhírterjesztés során is egyre nagyobb, napjainkra már kimagaslónak mondható jelentőségre tett szert,[743] amely a technológia kártékony felhasználása elleni fokozott védekezést és az ilyen magatartások fokozott szankcionálását is szükségessé teszi. Emellett számos technológiai nagyvállalat fejlesztett már ki deepfake tartalmak azonosítását segítő megoldást, továbbá ezen megoldások egy része nyilvánosan is elérhető. Ezen megoldások lényegében folyamatosan a deepfake technológia fejlődésével igyekeznek lépést tartani.

A deepfake technológia kapcsán érdemes megjegyezni, hogy akár jóhiszemű, a társadalom számára adott esetben hasznosnak tekinthető felhasználásokról (például: egy politikus nyilvános kijelentéseit parodizáló videóanyag készítése), akár rosszhiszemű felhasználásról, illetve visszaélésekről van szó (például: az érintettet valamely szexuális vagy egyéb kompromittáló helyzetben feltüntető képi- vagy videóanyag), személyes adatok kezelésére kerül sor, amennyiben a deepfake technológiával készült tartalom útján valamely természetes

[741] Emily FLITTER, Stacy COWLEY, Voice Deepfakes Are Coming for Your Bank Balance, *New York Times*, 2023.08.30., https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
[742] VESZELSZKI Ágnes: Deepfake: kételkedés a kételyben. In: ACZÉL Petra, VESZELSZKI Ágnes (szerk.): *Deepfake: a valótlan valóság*. Budapest, Gondolat Kiadó, 2023. 23.
[743] ESZTERI Dániel: A deepfake-technológia adatvédelmi értékelése a GDPR tükrében. In: ACZÉL Petra, VESZELSZKI Ágnes (szerk.): *Deepfake: a valótlan valóság*. Budapest, Gondolat Kiadó, 2023. 140.

személy azonosítható, vagy amennyiben a deepfake tartalmak előállításához (például: az adott megoldás fejlesztéséhez) személyes adatokat használnak. E tekintetben annak sincs jelentősége, hogy például egy deepfake felvételen megjelenő érintett a valóságban nem követett el olyan cselekményt vagy nem tett olyan kijelentést, amely az adott felvételen megjelenik, tekintettel arra, hogy a személyes adatnak nem szükséges valósnak vagy igaznak lennie, pusztán – a GDPR megközelítését alkalmazva – az érintettet közvetlen vagy közvetett módon azonosítania.[744] Ilyen esetekben azonban az adatkezelésre vonatkozó jogszabályi rendelkezéseknek is szükséges lehet megfelelni, amely a technológia fenti sajátosságai okán nehezen teljesíthető kihívásnak tekinthető.

Érdemes megemlíteni továbbá, hogy a technológia jóhiszemű felhasználása kapcsán alapjogok ütközése is felmerülhet. Így például a személyes adatok védelméhez fűződő jog jellemzően a szólás- és véleménynyilvánítás szabadságához fűződő joggal ütközhet (például: parodisztikus vagy szatirikus tartalmak elkészítése). Ilyen esetekben a szólás- és véleménynyilvánítás szabadsága elsőbbséget élvezhet, különösen amennyiben a technológia alkalmazása közszereplők nyilvános szereplésére vagy közhivatal betöltőjének bírálhatóságára vonatkozik. Elsőbbséget élvez azonban a személyes adatok védelméhez fűződő jog, amennyiben közvitához, közbeszédhez nem tartozó, különösen amennyiben rosszhiszemű, az érintett magánéletére fókuszáló tartalmakról van szó. Az internetes vitákban, egyes hozzászólásokban vagy tartalmakban azonban a magánélet es egyéb személyiségi jogok megsértésének lehetősége jellemzően nagyobbnak tekinthető, mint a sajtó vagy média útján tett nyilatkozatok esetén.[745] Míg ugyanis utóbbi esetén szerkesztői felelősség mellett készített es publikált tartalmakról beszélünk, előbbi esetben gyakran anonim, vagy nehezen azonosítható személyek állnak ad-hoc készült vagy impulzusszerű megnyilvánulásokat megjelenítő tartalmak mögött. Így az online diskurzusban, különösen az adott platformokon, weboldalakon tett nyilatkozatok, kommentek eseten felmerülhet az adott szolgáltató felelőssége is a vonatkozó tartalmakért, amelynek akar adatvédelmi vonatkozása is lehet. E körben azonban az adott megjegyzések, tartalmak által érintett személy magatartása,[746] valamint statusa, ismeretsége, az adott tartalmak tényszerű vagy vélemény jellege is jelentőséggel bírhat.[747] Igy adott esetben egy deepfake tartalom jogszerű megjelenítése, további felhasználása többféle szempont figyelembevételét

[744] GDPR 4. cikk 1. pontja
[745] Delfi v. Estonia, no. 64569/09, 2015. június 16-i ítélet, 133. bek.
[746] Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, no. 22947/13, 2016. február 2-i ítélet, 83. bek.
[747] Egill Einarsson v. Iceland, no 24703/15, 2017. november 7-i ítélet, 50. bek.

várja el (például: adatvédelmi, egyéb személyiségi jogi, felelősségi szempontok, az adott tartalom szellemi tulajdonjogi megítélése), amelyek kapcsán az alábbiakban a deepfake technológia MI Rendelet általi szabályozására es annak adatvedelmi hatásaira fokuszálunk.

Tekintettel a deepfake technológia egyre nagyobb jelentőségére, az MI Rendelet is szabályokat tartalmaz az ilyen tartalmak felhasználása kapcsán. Az MI Rendelet értelmében deepfake-nek minősül „*az MI által generált vagy manipulált kép, audio- vagy videotartalom, amely hasonlít létező személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és amely egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnne*”.[748] Így az MI Rendelet nem kizárólag a természetes személyekhez köthető tartalmakra vonatkozik, azonban adatvédelmi szempontból értelemszerűen a természetes személyeket azonosító deepfake tartalmak tekinthetők relevánsnak.

Hangsúlyozandó, hogy az MI Rendelet értelmében a szintetikus tartalmakat létrehozó MI-rendszerek szolgáltatóinak biztosítaniuk kell, hogy az MI-rendszer kimeneteit géppel olvasható formátumban jelöljék meg, és azok mesterségesen létrehozottként vagy manipuláltként észlelhetők legyenek. Ennek kapcsán a szolgáltatóknak megfelelő műszaki megoldásokat kell biztosítania, figyelembe véve a különböző tartalomtípusok sajátosságait és korlátait, a megvalósítás költségeit és a technika általánosan elismert állását. Ezen követelmények azonban nem alkalmazandók a hagyományos szerkesztési célú, illetve a bemeneti adatokat vagy azok szemantikáját lényegesen meg nem változtató támogató funkciót betöltő rendszerekre, illetve egyes bűnügyi célból alkalmazott rendszerekre.[749]

Emellett az olyan MI-rendszerek alkalmazói, amelyek eredetinek vagy valóságosnak tűnő deepfake tartalmakat hoznak létre vagy manipulálnak, kötelesek tájékoztatást nyújtani arról, hogy az adott tartalmat mesterségesen hozták létre vagy manipulálták. Mindez nem vonatkozik a jogszabályi felhatalmazáson alapuló bűnügyi célú alkalmazásra, illetve arra, ha a tartalom nyilvánvalóan művészeti, kreatív, szatirikus, fiktív vagy hasonló mű vagy program részét képezi – ez esetben csak olyan formában szükséges a fentiek szerinti tájékoztatást nyújtani, amely nem akadályozza az ilyen tartalmak megjelenítését vagy élvezetét. A deepfake tartalmakkal kapcsolatos tájékoztatási kötelezettség irányadó továbbá a közérdekű ügyekről való tájékoztatás céljából közzétett szöveget generáló vagy manipuláló MI-rendszer

[748] MI Rendelet 3. cikk (60) bek.
[749] MI Rendelet 50. cikk (2) bek.

alkalmazóira is, ide nem értve a jogszabályi felhatalmazáson alapuló bűnügyi célú alkalmazásra, illetve az emberi felülvizsgálaton vagy szerkesztési ellenőrzésen átesett tartalmak esetén, amennyiben a tartalom közzétételéért valamely természetes vagy jogi személy szerkesztői felelősséget visel.[750] Ennek értelmében tehát az MI Rendelet a közérdekű ügyekre vonatkozó robotújságírás kapcsán is transzparencia követelményeket határoz meg, amely segítséget jelenthet a dezinformáció és hírhamisítás elleni küzdelemben. Megjegyzendő azonban, hogy az MI Rendelet szerinti tájékoztatási kötelezettségnek (ideértve a deepfake tartalmakkal kapcsolatos tájékoztatási kötelezettséget is) való megfelelés nem mentesíti az alkalmazót az egyéb jogszabályok szerinti tájékoztatási kötelezettsége alól, ideértve adott esetben a GDPR szerinti tájékoztatást is.

Megjegyezzük, hogy habár az MI Rendelet fenti szabályai a deepfake társadalmi kockázatának lényegét helyesen ragadták meg azok csalárd, félrevezető jellegében, és a deepfake tartalmak ilyen mivoltáról való tájékoztatás előírása is az esetek jelentős részében hatékony megoldásnak tűnhet, azonban álláspontunk szerint tanácsos lett volna a deepfake felvételek rosszhiszemű felhasználása (például: csalások elkövetése vagy bosszúpornó) kapcsán az ilyen MI-gyakorlatok egyértelműen tiltott kategóriába sorolása, figyelembe véve, hogy az ilyen felvételek felhasználása (például: deepfake pornográf felvételek) jellemzően alapjaiban sérti meg az áldozatok emberi méltósághoz való jogát, illetve egyéb személyiségi jogait.[751] Az MI Rendelet jelenlegi szabályainak tükrében ugyanis kérdéses lehet, hogy például bizonyos deepfake tartalmak előállítása vagy felhasználása minősülhet-e tiltott gyakorlatnak, egy-egy ehhez használt rendszer milyen szempontok szerint tartozhat adott esetben magas kockázatú kategóriába, amely a gyakorlatban bizonytalanságokhoz vezethet.[752]

A deepfake tartalmak szabályozása kapcsán azonban az EU-n kívül is említhetők fejlemények. Így további pozitív példaként említhető Kalifornia állam szabályozása, ahol e körben két törvény is született. Az AB 730 törvény a politikai választások jogsértő befolyásolására használt tartalmakra vonatkozott (ideértve félrevezető, jogsértő tartalmak közzétételét választási

[750] MI Rendelet 50. cikk (4) bek.
[751] HERKE Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. *Pro Futuro*, 2023/13. 1. https://doi.org/10.26521/profuturo/2023/1/13334. 15.
[752] Felipe Romero MORENO: Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*, 2024. https://doi.org/10.1080/13600869.2024.2324540. 6.

befolyásolás céljából),[753] míg az AB 602 törvény a rosszindulatú, pornográf deepfake tartalmak felhasználása ellen vezet be szabályokat.[754] Megemlítendő, hogy 2023-ban New York állam is hasonló törvényt fogadott el, amely értelmében az érintett hozzájárulása nélkül róla jogsértő intim felvételek terjesztése, illetve közzététele – ideértve a mesterségesen generált deepfake tartalmakat is – bűncselekménynek tekintendő.[755] Emellett 2024-ben Tennessee államban is alkalmazandó egy „Elvis Act" elnevezésű törvény, amely az engedély nélküli deepfake tartalmak készítői mellett az ilyen tartalmak készítésére szolgáló megoldások kínálóit is szankcionálja.[756]

c. A biometrikus azonosító rendszerek alkalmazása

A közterületei kamerarendszerek telepítése önmagában is számos előnnyel járhat a társadalom, illetve az adott területen lakók számára, ideértve a biztonságos lakó- és munkakörnyezet garantálását, azonban értelemszerűen ennek kapcsán egyéb érdekek is felmerülhetnek, ideértve például az alapvető emberi jogok tiszteletben tartását.[757] A távoli biometrikus azonosítórendszerek, főként e körbe értve a különböző arcfelismerő rendszereket, lényegében a kamerarendszerek előnyeit és az alkalmazásukkal kapcsolatos kockázatokat is jelentős mértékben megnövelik.

A technológia jelentősége okán annak alkalmazásával kapcsolatban az MI Rendelet is szabályozza a valós idejű távoli biometrikus azonosító rendszereket, amely körébe tartozik az „*olyan távoli biometrikus azonosító rendszer, amelyben a biometrikus adatok rögzítése, az összehasonlítás és az azonosítás egyaránt jelentős késleltetés nélkül történik, nemcsak azonnali azonosítást megvalósítva, hanem – a kijátszás elkerülése érdekében – korlátozott rövid késleltetéseket is*".[758] Az MI Rendelet továbbá kitér a „nem valós idejű távoli biometrikus

[753] Assembly Bill No. 730, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730. Ezen jogszabály megújítás hiányában 2023. január 1. napjáig volt hatályban (section 1. 35. (b)).
[754] Assembly Bill No. 602, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB602
[755] New York State Assembly. S01042 Memo, https://nyassembly.gov/leg/?default_fld=%0D%0A&leg_video=&bn=S01042&term=2023&Summary=Y&Actions=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y
[756] Ensuring Likeness, Voice and Image Security (ELVIS) Act of 2024, https://legiscan.com/TN/text/HB2091/id/2900923
[757] KISS Attila: A közterületi térfigyelő rendszerek szabályozásának kihívásai a magyar jogalkotásban és a jogalkalmazásban. *Infokommunikáció és jog*, 2011/4. 136.
[758] MI Rendelet 3. cikk 42. pontja

azonosító rendszerre is, amely „a „valós idejű” távoli biometrikus azonosító rendszertől eltérő távoli biometrikus azonosító rendszer”.[759] Az MI Rendelet szövege kapcsán az egyik legvitatottabb pontot épp a valós idejű távoli biometrikus azonosító rendszerek szabályozása képezte, tekintettel az ezen rendszerek széleskörű használatával kapcsolatos jelentős társadalmi kockázatokra. Habár e körben a teljeskörű tilalom elrendelése sem tűnt sokáig lehetetlennek, nehéz vitatni, hogy a technológia bűnüldözési célú használatának teljes tilalma a hatóságok lehetőségeit is korlátozta volna az új technológiák bűnüldözési célú alkalmazása kapcsán, hiszen míg a bűnelkövetők az új technológiákat korlátozás nélkül használják, adott esetben kifejezetten bűncselekmények elkövetése céljából is, úgy az innovatív megoldások rendvédelmi alkalmazása már a vonatkozó jogszabályi rendelkezések által jelentős mértékben korlátozott.[760]

Hangsúlyozandó, hogy az MI Rendelet tiltja a „valós idejű” távoli biometrikus azonosító rendszerek használatát a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból, kivéve, ha arra a) emberrablás, emberkereskedelem vagy szexuális kizsákmányolás konkrét áldozatainak felkutatása vagy eltűnt személyek utáni kutatás, b) természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás tényleges és valós vagy tényleges és előre látható veszélyének megelőzése, vagy c) súlyos bűncselekmények (amelyek legalább négyévi szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel sújtandók) elkövetőinek lokalizálása nyomozás vagy büntetőeljárás lefolytatása vagy büntetőjogi szankció végrehajtása céljából kerül sor.[761]

A „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő felhasználása esetén továbbá ezen rendszerek fentiek szerinti használata kizárólag a csak a konkrét célszemély személyazonosságának megerősítése érdekében indítható el, figyelembe véve a lehetséges használatot eredményező helyzet jellegét, valamint a rendszer használatának valamennyi érintett személy jogaira és szabadságaira gyakorolt következményeit.[762] Az ilyen rendszerek alkalmazásának továbbá megfelelő tagállami jogszabályi felhatalmazással szükséges rendelkeznie, illetve az a szerint

[759] MI Rendelet 3. cikk 43. pontja
[760] SZABÓ Hedvig: A mesterséges intelligenciára vonatkozó szabályozás, jogalkotás a rendvédelem tükrében. *MTA Law Working Papers*, 2023/16, https://jog.tk.hu/mtalwp/a-mesterseges-intelligenciara-vonatkozo-szabalyozas-jogalkotas-a-rendvedelem-tukreben?download=pdf. 10
[761] MI Rendelet 5. cikk (1) bek. h) pontja
[762] MI Rendelet 5. cikk (2) bek.

meghatározott keretek között alkalmazhatók, ideértve különösen az alkalmazás ideje, helye, illetve az érintettek köre szerinti korlátozásokat. Így jellemzően – a célhoz kötöttség alapelvével összhangban – csak a büntetőjogi felelősség megállapítása szempontjából releváns információk használhatók fel bizonyítékként,[763] az e körbe nem tartozó adatok kezelése pedig lehetőség szerint kerülendő, ennek hiányában pedig a nem releváns információk a bizonyítékok értékelésekor eltávolítandók. Az ilyen rendszerek kapcsán kiemelendő továbbá, hogy az azt alkalmazó hatóság köteles a rendszer alkalmazását megelőzően alapjogi hatásvizsgálatot végezni, valamint a rendszert a vonatkozó uniós adatbázisban regisztrálni. Kellően indokolt sürgős esetekben azonban a regisztráció később is elvégezhető.[764]

A „valós idejű" távoli biometrikus azonosító rendszer nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatára kizárólag megfelelően indokolt kérelem alapján, az alkalmazás szerinti tagállam illetékes igazságügyi hatósága vagy független közigazgatási hatósága – amelynek határozata kötelező erejű – által kiadott előzetes engedélye alapján kerülhet sor az irányadó nemzeti jogszabályi rendelkezések szerint. Kellően indokolt sürgős esetekben az alkalmazásra azonban sor kerülhet a fenti előzetes engedély hiányában is, feltételezve, hogy azt indokolatlan késedelem nélkül, de legkésőbb 24 órán belül kérik, annak megtagadása esetén pedig a használatot azonnali hatállyal leállítják, a vonatkozó eredmény, kimenet pedig haladéktalanul megsemmisítésre, törlésre kerül.[765]

A fentiek kapcsán kiemelendő, hogy a fenti hatóság az engedélyt akkor adhatja meg, amennyiben meggyőződött arról, hogy a rendszer használata a megkeresésben azonosított célok valamelyikének eléréséhez szükséges és azzal arányos, továbbá különösen, hogy az időtartam, valamint a földrajzi és személyi hatály tekintetében a feltétlenül szükséges mértékre korlátozódik. Emellett kiemelendő, hogy a „valós idejű" távoli biometrikus azonosító rendszer kimenete alapján nem hozható olyan döntés, amely egy személyre nézve kedvezőtlen joghatással jár.[766] Hangsúlyozandó azonban, hogy a tagállamok a „valós idejű" távoli biometrikus azonosító rendszer nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatára vonatkozóan – a fenti követelmények figyelembevételével – teljes vagy részleges jogszabályi felhatalmazást adhatnak, és ez esetben nemzeti jogukban rögzítik

[763] A Szegedi Ítélőtábla Pf.20282/2022/5. számú határozata [50]. bek.
[764] MI Rendelet 5. cikk (2) bek.
[765] MI Rendelet 5. cikk (3) bek.
[766] Uo.

engedélyek kérelmezésére, kiadására és felhasználására, valamint az azokkal kapcsolatos felügyeletre és jelentéstételre vonatkozó szükséges részletes szabályokat. A tagállamok továbbá a fenti szabályokról legkésőbb az azok elfogadását követő 30 napon belül értesítik a Bizottságot. A tagállamok jogosultak továbbá akár szigorúbb szabályok bevezetésére is,[767] adott esetben akár a távoli biometrikus azonosítási rendszerek alkalmazásának jelentős korlátozásával.

Emellett a „valós idejű" távoli biometrikus azonosító rendszer nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatáról az illetékes piacfelügyeleti hatóságot és adatvédelmi hatóságot is értesíteni kell, az ezzel kapcsolatos releváns információk továbbításával (ide nem értve érzékeny operatív adatokat),[768] amelyek az ilyen értesítésekről éves jelentést tesznek a Bizottság számára,[769] amely az ilyen tagállami jelentések alapján éves jelentést publikál a nyilvánosság számára.[770]

Hangsúlyozandó, hogy a fentiekhez hasonlóan a „nem valós idejű" távoli biometrikus azonosító rendszerek alkalmazása kapcsán bűncselekményt elkövetésével gyanúsított vagy már elítélt személy célzott felkutatására irányuló nyomozás keretében az ilyen azonosításra szolgáló, nagy kockázatú MI-rendszert alkalmazó személynek előzetesen vagy indokolatlan késedelem nélkül, de legkésőbb 48 órán belül engedélyt kell kérnie az adott rendszer használatára valamely igazságügyi hatóságtól vagy közigazgatási hatóságtól, amelynek határozata kötelező erejű és felülvizsgálat tárgyát képezi, kivéve az objektív és ellenőrizhető tényeken alapuló kezdeti azonosítására vonatkozó használat esetét. Az ilyen rendszerek használatának is továbbá a nyomozáshoz feltétlenül szükséges mértékre kell korlátozódnia, emellett az engedély elutasítása esetén a rendszer használatát azonnali hatállyal le kell állítani, a korábbi engedély alapján gyűjtött személyes adatokat törölni kell.[771]

Tekintettel a távoli biometrikus azonosító rendszerek alkalmazásával kapcsolatos kockázatokra, megemlítendő továbbá, hogy az elmúlt években több adatvédelmi felügyeleti hatóság is szabott ki bírságot arcfelismerő rendszerek alkalmazásával kapcsolatos jogsértő adatkezelés okán, ideértve például a Clearview AI megoldás alkalmazójával szembeni

[767] MI Rendelet 5. cikk (5) bek.
[768] MI Rendelet 5. cikk (4) bek.
[769] MI Rendelet 5. cikk (5) bek.
[770] MI Rendelet 5. cikk (6) bek.
[771] MI Rendelet 25 cikk (10) bek.

eljárásokat és jelentős szankciókat.[772] A technológiával járó adatvédelmi kockázatok súlyosságát jelzi a NAIH siófoki közterületen arcfelismerésre is képes kamerákat magában foglaló közterületi rendszer működtetése tárgyában indított adatvédelmi hatósági eljárása. Az eset során a hatóság sajtóhírekből értesült az esetleges arcfelismerő technológia alkalmazásáról, amelyet követően eljárást indított az üzemeltetőkkel szemben. Ugyan az eljárás során nem nyert bizonyítást az arcfelismerő technológia alkalmazása, a NAIH azonban több jogsértést is megállapított (ideértve az adatkezelői szerepkörök bizonytalanságát, adatbiztonsági intézkedések elégtelenségét), amelyekre tekintettel bírság kiszabásáról, valamint a döntése rendszer üzemeltetésében résztvevő entitások megnevezésével való publikálásáról döntött.[773]

A fentieken túl az ilyen rendszerek megfelelő szabályozását feltételezve álláspontunk szerint kiemelten fontosnak tekinthető az adott rendszer előzetes tesztelése. Ez optimálisan több lépésben történhet, például először zárt területen, kizárólag erre jelentkező tesztalanyok részvételének biztosításával, még egy következő lépésben egy kevéssé frekventált nyilvános területen, végül a megfigyeléssel kapcsolatos célterületen. Ennek során hatékonyan felmérhetők a rendszer esetleges hibái, azon körülmények vagy szempontok, amelyek további értékelést vagy finomítást tesznek szükségessé, ezek dokumentálásával pedig a rendszer későbbi fejlesztése, karbantartása is nagyban segíthető.

Természetesen a megfelelő előzetes tesztelésen túl fontos az ilyen nagy kockázatú rendszerek megfelelő időközönként való felülvizsgálata, az esetlegesen jelzett hiányosságok, visszaélések haladéktalan áttekintése és kiértékelése, és a szükséges körű javító célú intézkedések megtétele. Így értelemszerűen nem elegendő, ha a rendszer az alkalmazás kezdetekor megfelelően működik, azonban hosszú ideig érdemi felülvizsgálat nélkül marad. Szükséges ugyanis a rendszeres, dokumentált felülvizsgálat elvégzése, az adatvédelmi és egyéb irányadó jogszabályi rendelkezésekkel összhangban. Emellett ki kell dolgozni, és biztosítani kell az érintettek jogai érvényesítésének támogatását célzó módszereket, ezeket továbbá szükségesnek tűnik összhangba hozni azon eljárások (például: büntetőeljárás, szabálysértési eljárás vagy egyéb hatósági eljárások) szabályaival, ahol a technológiát, illetve az az által rögzített felvételeket, egyéb adatokat felhasználják.[774] Kiemelten fontosnak tekintendő továbbá, hogy az adott

[772] Lásd: az adatkezelés ellenőrzésével foglalkozó fenti pontban a Clearview AI-al szembeni eljárások kapcsán írtak.
[773] NAIH-963-10/2022. 18-21.
[774] NECZ Dániel: A mesterséges intelligencia belügyi és biztonsági célú alkalmazása. *Scientia et Securitas*, 2020/1. 1. 51.

rendszer csak megfelelő célból kerüljön alkalmazásra a megfigyelés által érintett területen, időszakban, illetve személy kapcsán, az ilyen megfelelő céllal, illetve az ezen technológia alkalmazásával össze nem egyeztethető további etikátlan célokból távoli biometrikus azonosítás nem végezhető. Ennek kapcsán negatív példaként említhető az Egyesült Államokban, a Madison Square Garden rendezvényhelyszín üzemeltetői által történő arcfelismerő technológia használat, amelynek során állítólagosan az üzemeltetőket perlő ügyvédi irodák munkatársait azonosították a területre való bejutás meggátolása érdekében.[775]

A fentiek kapcsán természetesen nehéz vitatni a technológia alkalmazásával járó veszélyeket. Nehéz meghúzni azt a határt, ahol a távoli biometrikus azonosító rendszerek alkalmazása egy demokratikus társadalomban szükséges és indokolt lehet. Amennyiben például egy adott közterületen alkalmazott rendszer segítségével könnyebben azonosíthatók és vonhatók felelősségre a zsebtolvajok, az kétségtelenül előnyökkel is jár a társadalom számára (ideértve például a közbiztonság növelését vagy a bűnüldözés hatékonyságát), azonban feltételezi, hogy az adott, jellemzően nagyszámú ember által gyakran látogatott területen folyamatos, arcfelismeréssel járó megfigyelése történik, az ezen területen elhaladó érintetteket pedig az MI-rendszer akár viszonylag kisebb súlyú bűncselekményekkel összefüggésben is azonosíthatja. Mindez például a gyülekezési jog, illetve a véleménynyilvánítási jog gyakorlása szempontjából is elrettentően hathat, és a totális megfigyeléstől való félelemérzetet alakíthat ki az állampolgárokban. Mindez értelemszerűen a társadalom számára jelentős kockázatokkal járhat, ugyanis tömeges megfigyelést alapoz meg, illetve az „egyszerű" térfigyelő kameráknál kifinomultabb, komplexebb azonosítást, értékelést lehetővé tevő megoldással, így akár egyes csoportok is könnyebben diszkriminálhatóvá válnak, a megfigyelés pedig akár a városszervezésre is hatással lehet.[776]

Minderre tekintettel a fentiek kapcsán érthetőnek tekinthetők a technológia alkalmazásával kapcsolatos aggályok és a vonatkozó korlátozások. Hangsúlyozandó azonban, hogy nem kizárólag a súlyos bűncselekmények elkövetőinek vagy feltételezett elkövetőinek azonosítása lehet az egyetlen olyan terület, ahol a technológia sikeresen alkalmazható. Így például eltűnt személyek, sérült vagy más magatehetetlen emberek is könnyebben megtalálhatók a

[775] Zach WILLIAMS: NY AG Tish James bashes MSG facial surveillance as 'plagued' with legal problems. *New York Post*, 2023.01.25, https://nypost.com/2023/01/25/ag-letitia-james-demands-docs-from-msg-about-facial-surveillance-of-legal-enemies/

[776] Andrea PIN: Artificial Intelligence, the Public Space, and the Right to be Ignored. In: Alberto QUINTAVALLA, Jeroen TEMPERMAN (eds.): *Artificial Intelligence and Human Rights*. Oxford University Press, 2023. 189.

segítségével. Ezen esetekben a téves azonosítás is jellemzően kevesebb káros hatással járhat az érintettekre nézve, és sokszor a megfigyelés által érintett terület is szűkebb körű vagy kevésbé frekventált lehet (például: elhagyatott vagy lakatlan területek).

Megemlítendő továbbá, hogy a biometrikus azonosítási technológia a közterületi megfigyeléssel kapcsolatos alkalmazáson túl számos egyéb módon is alkalmazásra kerülhet, például közösségi média profilok vagy az interneten elérhető fénykép- és videófelvételek elemzésére, segítségükkel ugyanis az érintett megfigyelése, jellemzőinek és viselkedésének értékelése is jóval hatékonyabban végezhető, sok esetben az érintett számára sérelmes, magánéletébe túlzó behatást engedő módon. Egy 2017-ben végzett kutatás szerint például az MI képes volt akár egyetlen kép alapján is helyesen azonosítani a férfiak 81%-ának, illetve a nők 74%-ának szexuális irányultságát.[777] Emellett azonban az arcfelismerő rendszerek az emberi tulajdonság és viselkedés számos egyéb aspektusát képesek az emberi szemlélőnél hatékonyabban felismerni, valamint értékelni, amelyek adatvédelmi szempontból további kihívásokhoz vezethetnek. Ezeket továbbá gyakran kontextus nélkül, pusztán egy-egy jellemzőre fókuszáltan teszik, amely adott esetben diszkriminatív gyakorlatok kialakítását, illetve az ezzel kapcsolatos társadalmi igazságtalanságokat is felerősítheti.[778] Ezen veszélyekre tekintettel a biometrikus azonosítási rendszereket általában nagy kockázatúnak minősíti az MI Rendelet, ide nem értve a jellemzően kevesebb kockázattal bíró, kizárólag az érintett személyazonosságának igazolására szolgáló rendszereket.[779]

7. A mesterséges intelligencia kapcsán szükséges-e újra gondolnunk a személyes adatok védelmét?

Az MI rohamos fejlődése és elterjedése kapcsán felmerülhet a kérdés, hogy szükséges-e újra gondolnunk a személyes adatok védelmét. Az MI és az ezzel kapcsolatos technológiák (például: egyes okos egészségügyi megoldások, chatbot alkalmazások, stb.) robbanásszerű fejlődést produkáltak az elmúlt években, a fejlődés üteme pedig egyre inkább csak gyorsulni látszik. Mindez egyben a társadalomra és a gazdaságra is jelentős hatással bír, és újabb, korábban csak

[777] Yilun WANG, Michael KOSINSKI: Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, vol. 114, issue 2. (2018). https://doi.org/10.1037/pspa0000098. 250.
[778] Kate CRAWFORD: *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, London, Yale University Press, 2021. 94.
[779] MI Rendelet III. sz. mellékletének 1. pontja

a tudományos-fantasztikus művek lapjain vagy a filmvásznon látott, egyre kevésbé futurisztikusnak tűnő élethelyzeteket eredményez. Néhány évtizede például ki gondolta volna, hogy a nagy nyelvi modellek forradalmasítják majd a munkavégzést, valamint számos iparágat, vagy hogy egy képgeneráló megoldás néhány másodperc alatt képes lesz világhírű festőművészekhez hasonlóan szemet gyönyörködtető képeket alkotni. Már nem vagyunk messze attól a korszaktól, amikor az MI vezérli majd a városok üzemeltetését, a közlekedést és a gyártást, valamint a mindennapjaink nagy részét is. Az MI segít majd minket munkahelyünkön, fogad minket az otthonunkban egy fárasztó nap végén, és az MI segítségével töltjük majd el a szabadidőnket is, például egy egészestés hollywood-i filmet létrehozva a főszereplésünkkel – ez utóbbi jelenség már napjainkban is felsejleni látszik. Így az OpenAI által 2024. elején beharangozott SORA nevű megoldása például képes szöveges utasítások alapján akár teljesen élethű, illetve filmszerű, rövid videótartalmakat generálni.[780] Erre a robbanásszerű fejlődésre nyilván a jognak is reagálnia kell. Egyelőre azonban inkább a hatósági jogalkalmazás dominanciájáról beszélhetünk, ahol az általános adatvédelmi követelményekre tekintettel próbálják az adatvédelmi hatóságok „irányba terelni" az MI általi adatkezelést. Erre jó példának tekinthető az olasz adatvédelmi hatóság 2024. márciusában indított eljárása, amely során a Sora lehetséges alkalmazására tekintettel kérdéseket intézett az OpenAI-hoz, a modell kapcsán személyes adatok gyűjtésére és felhasználására fókuszálva.[781]

Az MI adatéhsége és a Big Data-alapú adatkezelések sokasága, az MI által folytatott adatkezelések komplexitása, valamint az általános célú MI-modellek elterjedése és sokoldalúsága megkérdőjelezni látszanak az adatvédelemi alapelvek tarthatóságát, az átláthatósággal és a hozzájárulással kapcsolatos jelenlegi adatvédelmi szabályozáshoz, követelményekhez való ragaszkodás további lehetőségét.[782] Természetesen egyes szabályozási megközelítések – sok szempontból helyesen, technológiasemleges módon – az esetleges változásokra felkészülten próbálnak reagálni a fenti beláthatatlannak tűnő változásokra. Ezen megközelítést alkalmazza a GDPR is. Az adatvédelmi szabályozás minden aspektusa azonban értelemszerűen nem lehet általános vagy technológiasemleges, bizonyos technológiák vagy azok egyes területen való felhasználása kapcsán pedig szükség van technológia-specifikus szabályozási megoldásokra is. Így a termékfelelősségi logikára építő MI Rendelet is sok esetben

[780] Lásd: OpenAI, SORA, https://openai.com/sora
[781] Garante, Intelligenza artificiale, il Garante privacy avvia istruttoria su "Sora" di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9991867
[782] Ződi (2017) i. m. 27.

specifikus felelősségi szabályokat határoz meg az MI-rendszerek kapcsán, és az amerikai vagy más harmadik országbeli szabályozási modellek is sok esetben ezt a technológia-specifikus megközelítést követik (például: a deepfake technológia kapcsán az USA egyes tagállamai által alkotott törvények). Mindez azért is fontos, mivel az MI általi adatkezelés (ideértve például az algoritmusok általi értékeléseket) nem tekinthető statikus folyamatnak, az sokszor az adatok újbóli értékelésével, további feldolgozásával jár, amely folyamatok állandó figyelemmel kísérése nem várható el az érintettektől.[783] Mindazonáltal az MI-rendszerek szolgáltatóitól, illetve alkalmazóitól sem várható el, hogy az érintettet a számára csekély hatással járó technikai műveletekről is tájékoztassák, így az adatvédelmi szabályozás jelenlegi, sok esetben statikusnak tekinthető, az adatkezelési műveletek jelentős része kapcsán egységes követelményeket támasztó megközelítése helyett szükségesnek tűnik a kockázat-alapú megközelítés fokozott alkalmazása, az adatkezelés tényleges hatásaira való koncentrálás.

A magunk részéről ennek kapcsán példamutatónak tekintjük az MI Rendelet kockázatalapú megközelítését, amely javarészt arányosan igyekszik reagálni az egyes MI-rendszerekre, valamint azok alkalmazásával kapcsolatos kockázatokra, a szabályozás adatvédelmi, szellemi tulajdonjogi és egyéb specifikus jogterületekkel való összhangja azonban napjainkban még nem biztosított, ezen jogterületek kérdéseinek megválaszolását pedig általánosságban az MI Rendelet nem is célozza. Emellett az EU-n belül egy fragmentált szabályozás alakult ki a digitális piacok területén, amely jelentős számban tartalmaz transzparenciával, adattovábbítással, felhasználói jogok biztosításával kapcsolatos követelményeket, ezek érvényesíthetősége, adatvédelmi szempontjai azonban egyelőre kevéssé ismertek, és fennáll a veszélye, hogy az, érintettek számára, az adatokhoz való hozzáféréssel, azokkal való rendelkezéssel kapcsolatos jogok, illetve a transzparenciával kapcsolatos követelmények jelentős részben a szolgáltatók dokumentációs kötelezettségeivé redukálódnak.

Egyes területeken azonban a jelenlegi követelmények enyhítésére lenne szükség, különösen olyan esetekben, ahol az MI alkalmazása kiemelt lehetőségeket rejt magában, és a társadalom számára különösen jelentős eredményekhez vezethet (például: az egészségügyi kutatások területén). Az ilyen adatkezelések kapcsán az EU-n belül a GDPR bizonyos szintű enyhítést

[783] Hideyuki MATSUMI, Daniel J. SOLOVE: *The Prediction Society: AI and the Problems of Forecasting the Future*. GWU Law School Public Law Research Paper No. 2023-58. (2024). https://ssrn.com/abstract=4453869, http://dx.doi.org/10.2139/ssrn.4453869. 49.

biztosít,[784] azonban számos egyéb követelmény (például: a célhoz kötöttség vagy az adatminimalizálás általános, alapelvi követelménye) adott esetben az enyhítést célzó szabályok ellenére is jelentős korlátozást jelenthet az MI általi adatkezelések kapcsán. Mindez azért is fontos, mivel az európai kontinens kiemelkedő jelentőségű kutatóhálózatokkal rendelkezik, amelyek nagyobb mértékű bevonása az MI kutatásokba jelentős mértékben hozzájárulhatnak a társadalmi és gazdasági fejlődéshez.[785] Megjegyzendő azonban, hogy az adott esetben társadalmilag hasznosnak tekinthető adatkezelési cél sem jelenthet mindig felmentést az alapvető adatvédelmi követelmények alól. Így például az olasz adatvédelmi hatóság 2024-ben arra a megállapításra jutott, miszerint a trentói önkormányzat jogsértően járt el, amikor kutatási célból engedélyezte egy szervezetnek, hogy a városban hang- és képfelvételeket gyűjtsön a közbiztonságot veszélyeztető helyzetek hatékonyabb azonosítása érdekében.[786] Ettől függetlenül a GDPR jelenlegi szabályai sok esetben látszólag egyszerre jelentenek korlátozást a hasznos és a kártékonynak tekinthető adatkezelések számára.

Az MI kapcsán továbbá számos, alapvető adatvédelmi követelménynek való megfelelés is nehezen biztosíthatónak tűnik. Például, hogyan tud egy interneten elérhető információkra támaszkodó általános célú MI-rendszer célhoz kötötten működni, vagy hogyan minimalizálhatja az általa gyűjtött adatokat? Mennyire alkalmazható átláthatóan az alkalmazása által érintett valamennyi személy számára? Az újabb és újabb innovatív megoldások idővel vélhetőleg csak még inkább szétfeszítik a jelenlegi szabályok alkalmazhatóságát, értelmezhetőségét. A jelenlegi szabályok tükrében megoldást kínálhat bizonyos adatvédelmi követelmények gyakorlati szempontú „áthangolás", ideértve például az érintettek tájékoztatását. A tájékoztatásnak természetesen az érintettek számára átlátható adatkezelést szükséges garantálnia az MI-rendszerek alkalmazása esetén is, azonban célravezető lehet egy olyan, a jelenleginél megengedőbbnek tekinthető megközelítés, ahol a technológia alkalmazásával kapcsolatos „észszerűen várható bizonytalanságok" beépülnek a megfelelő tájékoztatási gyakorlatba. Például az MI orvosi célú alkalmazása esetén – önmagában az MI-rendszer alkalmazásának eredménye alapján – nem feltétlenül adható teljeskörű tájékoztatás arról, hogy az MI miért azonosított egy adott megbetegedésre való hajlamot bizonyos

[784] Ideértve például a GDPR 9. cikk (2) bekezdése szerinti, a különleges adatok általános tilalma alóli egyes kivételek vagy a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból végzett adatkezelések, amelyeket a GDPR az eredeti céllal alapvetően összeegyeztethetőnek tekint (GDPR 5. cikk (1) b) pontja).
[785] PALKÓ Tamás: A mesterséges intelligencia kutatása az Európai Unióban. *Európai Jog*, 20/4, 2020. 21.
[786] Garante, Provvedimento dell'11 gennaio 2024 [9977020], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020. 4.

százalékban az adott betegnél. Azonban a megfelelő orvosi tájékoztatással karöltve adott esetben a fenti bizonytalanságokkal „terhelt" adatvédelmi tájékoztatás is elégséges lehet, az MI által hozott döntés okai pedig emberi közreműködéssel adott esetben kivizsgálhatók. Megemlítendő azonban, hogy bár a fenti „rugalmas" értelmezés álláspontunk szerint akár a GDPR jelenlegi szövegéből is levezethető lenne, a jövőben az MI alkalmazásával és az MI általi adatkezeléssel kapcsolatos átláthatóságra vonatkozó követelményeknek is egységesen kellene érvényesülniük az EU-n belül, a tagállami hatóságok és bíróságok „jóindulatú" eseti értelmezésében való bizakodás helyett. Egyértelmű és egységesen alkalmazott átláthatóságra vonatkozó követelmények hiányában ugyanis az adott esetben eljáró hatóságok, bíróságok mellett az érintett szolgáltatók, adatkezelők kell, hogy meghatározzák az átláthatóság kereteit, amely félreértésekre, valamint manipulációra is alapot adhat.[787]

Megemlítendő továbbá, hogy az MI Rendelet nem hoz létre önálló jogalapokat az MI általi adatkezelésre, és nem írja felül az adatkezelés alapelveit sem. Ettől függetlenül álláspontunk szerint az MI általi adatkezelés kapcsán jelentős lehetőséget biztosíthat az eredeti adatkezelési céllal összefüggő adatkezelésre hivatkozás.[788] Ez különösen olyan esetekben alkalmazható, ahol az MI alkalmazása szorosan kapcsolódik egy korábbi adatkezeléshez, és azt mintegy kiegészíti vagy támogatja. Így az eredeti céllal összefüggőnek minősülhet például egy előadásról készült hang- vagy videófelvétel kapcsán – feltéve, hogy azt az érintett hozzájárulásával, vagy egyébként jogszerűen rögzítették – olyan MI-rendszer alkalmazása, amely az előadás lényegét összefoglalja, segítséget nyújtva például tudományos konferenciákon, üzleti eseményeken elhangzottak vagy újságírók által készített interjúk pontosabb rögzítésére. Ilyen esetekben az adatkezelőtől elvárható lehet adott esetben további intézkedések alkalmazása is, amely az érintettekre nézve az esetleges hátrányos következményeket csökkenti[789] (például: az MI-rendszer által készített összefoglalás interjú alanyával történő egyeztetése, az esetleges hibásan rögzített részek emberi felülvizsgálata).

A fentiek tükrében meglátásunk szerint az MI általi adatkezelés kapcsán – a teljesség igénye nélkül, az álláspontunk szerint legjelentősebbnek tekinthető gyakorlati problémák azonosítása

[787] Heike FELZMANN, Eduard FOSCH VILLARONGA, Christoph LUTZ, Aurelia Tamò LARRIEUX: Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big *Data & Society* 6/1. (June 2019). https://doi.org/10.1177/2053951719860542. 10.
[788] GDPR 6. cikk (4) bek.
[789] GDPR 6. cikk (4) bek. d) pontja

mellett – különösen az alábbi szempontok érvényesítése támogathatja leginkább a technológia felelős alkalmazását, valamint az innováció fejlődését:

- az adott szolgáltató piaci hatalmával, társadalmi befolyásával, valamint a fentiekkel összefüggésben a felhasználók számával és tevékenységével,[790] kapcsolódó adatkezelések jelentőségével összhangban álló felelősségi szabályok meghatározása;
- a túlzott protekcionizmus elkerülése, ehelyett az innovációra és a lehetséges körű együttműködésre való koncentrálás;
- az MI elengedhetetlen vagy társadalmilag hasznos területeken való alkalmazásának támogatása;
- a káros tartalmak es alkalmazási módok megfelelő elkülönítése es kezelése (ideértve például a deepfake tartalmak zsarolási célú felhasználását).[791]
- az MI alkalmazásával, valamint a felhasznált adatokkal, alkalmazott technológiával kapcsolatos „arányos átláthatóság" biztosítása;
- kockázatalapú megközelítés a személyes adatok védelme kapcsán is, amely elsődlegesen az adatkezelés érintettre gyakorolt hatásait veszi alapul;
- a diszkrimináció és más, az érintettek érdekeit aránytalan módon sértő megoldások alkalmazásának elkerülése, e tekintetben jó gyakorlatok, szempontrendszerek meghatározása (például a tanítóadatok reprezentativitása terén);
- a túlzott félelmek és indulatalapú szabályozás helyett az etikus MI alapkövetelményeinek érvényesítése.

A fentiekre tekintettel elsődlegesnek tekinthető az innovációt és a fejlesztéseket támogató szabályozási környezet kialakítása, amely e körben az érintettek és a szolgáltatók, alkalmazók észszerű elvárásait is figyelembe veszi, és e körben arányos és észszerű követelményeket támaszt az új technológiák szolgáltatóival, alkalmazóival szemben. Ez utóbbi tekintetben relevánsak lehetnek például gazdasági vagy információbiztonsági szempontból jelentős információk, adatkészletek kiaknázását védő szabályok.[792] Emellett a fentebb említett „arányos átláthatóság" körében adandó tájékoztatásnak az MI általi adatkezelések kapcsán álláspontunk szerint elsősorban az érintettre járó vagy az érintett és a környezete számára releváns hatásokra kell fókuszálnia az adatkezelés részletes ismertetése helyett, tekintettel arra, hogy a „túlzott"

[790] TÓTH (2018) i.m. 52.
[791] MORENO op. cit. 7.
[792] Necz (2022a) i.m. 15.

transzparencia vagy a formális tájékoztatás is félrevezethetik az érintettet és erodálhatják a transzparens adatkezelés előnyeit.

Kiemelendő, hogy technológia környezetben értelemszerűen az érintetti joggyakorlás is jellemzően sajátosan foghat helyt. E körben álláspontunk szerint kiemelt hangsúllyal bír majd az MI-rendszerek szolgáltatóinak, alkalmazóinak az érintetti jogok gyakorlásának támogatására kialakított gyakorlata, megközelítése. Ezen megközelítések különösen kiszolgáltatott érintetti kör esetén bírhatnak jelentősebb hangsúllyal, ahol az adatkezelőknek hatékonyabb intézkedések útján szükséges az érintetti joggyakorlást támogatniuk. Így például gyermekek, kórházi ellátásra szoruló betegek esetén magasabb szintű támogatás várható el az adatkezelőtől, hiszen ezen személyek értelemszerűen kevésbé lehetnek képesek jogaikat gyakorolni, érdekeiket érvényesíteni.

A fentieken túl álláspontunk szerint a szabályozásnak nagyobb figyelmet kell fordítania a diszkrimináció és a társadalom számára jelentős hátránnyal járó egyéb hatások meggátolására is, a visszaélések kiszűrésére, és a magas fokú információbiztonságra tekintettel. E körben azonban álláspontunk szerint az adatvédelmi követelményeknek kockázatalapú megközelítést követve, az adott rendszer kockázatával arányos mértékben kell érvényesülniük, a technológiával kapcsolatos túlzott félelmek helyett pedig az etikus felhasználás kell, hogy nagyobb hangsúlyt kapjon. Erre tekintettel a közeljövőben vélhetőleg nagyobb jelentőséggel bír majd az egyes szakmai és gazdasági szervezetek önszabályozói gyakorlata, valamint az adott iparág vagy szakma szereplői többsége által követett etikus gyakorlatok.

8. Záró gondolatok

Az MI-rendszerek kiterjedt alkalmazása jelentős kihívás elé állítja a személyes adatok védelmét, ideértve a jelentős adatmennyiség felhalmozására, hasznosítássa épülő gazdasági modelleket és új technológiai megoldásokat.[793] Ezen új környezet azonban új lehetőségeket is biztosít az MI rendszerek szolgáltatóinak és alkalmazóinak, a digitális piacok szereplőinek. Napjainkban ugyanis az online szolgáltatások piacán aktív vállalkozások egyre jelentősebb szerepet játszanak az információáramlás szabályozásában, valamint az adatok

[793] SZŐKE Gergely László: Az adatvédelem szabályozásának történeti áttekintése. *Infokommunikáció és jog*, 2013/3. 110.

felhasználásában, így ezen új szerepkörhöz vagy hatalomhoz ezzel arányos felelősség és jogok társítandók.[794] Mindez különösen igaz az MI elterjedése kapcsán, ugyanis a közösségi médiaszolgáltatók, a keresőszolgáltatást nyújtók és az adatgazdaság további szereplőinek befolyása a társadalmi folyamatokra az elmúlt években csak még hangsúlyosabbá vált. E tekintetben nem feltétlenül kizárólag az adott tartalmak megtekintői, az adott alkalmazás vagy szolgáltatás felhasználóinak száma hanem inkább azok a társadalmi és gazdasági hatások számítanak, amelyeket az adott szolgáltatás, weboldal vagy alkalmazás kivált vagy észszerűen kiválthat.[795]

A fentiek kapcsán megemlítendő továbbá, hogy nemzetközi szinten habár az MI-vel kapcsolatban számos elvi iránymutatás, alapvető követelményrendszer látott már napvilágot, ezen sok esetben nélkülözik a vállalkozások számára is értelmezhető emberi jogi követelményeket, emellett az EJEB vagy egyéb nemzetközi bíróságok is jellemzően kevéssé tárgyaltak eddig MI fókuszú emberi jogi ügyeket, habár ezen fórumokon az adatvédelem jellemzően kiemelt hangsúllyal bír.[796] Emellett az egyes országok és régiók eltérő szabályozási technikákat alkalmaznak az adatvédelem és az MI szabályozása területén, amelyek különböző mértékben hatnak a technológiai fejlődésre és az egyes technológiák alkalmazására. Megemlítendő azonban, hogy mind az adatvédelmi, mind az MI szabályozás területén az EU vezető szereppel rendelkezik, szabályozási megoldásai pedig egyben mintaként is tekinthetők harmadik országok számára. Mindez segíthet csökkenteni az eltérő szabályozásból származó nehézségeket (például az adatok határon átnyúló továbbítása, közös adatkezelési műveletek folytatása terültén).

Leszögezendő továbbá, hogy az MI Rendelet alapvetően kockázatalapú megközelítésből indul ki, amely az adott rendszer által jelentett kockázatok szerint támaszt tilalmakat vagy rendel követelményeket. Mindez az átfogó európai adatvédelmi szabályozással karöltve széleskörű védelmet biztosíthat az érintettek számára, amely különös figyelmet helyez az átláthatóságra, az érintetti jogok gyakorlásának támogatására és biztosítására, valamint a megfelelő szintű adatbiztonsági intézkedések bevezetésére és fenntartására. Egyúttal azonban az MI Rendelet

[794] MENYHÁRD Attila: A magánélet védelme az Emberi Jogi Bíróság gyakorlatában. In: GÖRÖG Márta, MENYHÁRD Attila, KOLTAY András: *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül*. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017. 62.
[795] KOLTAY András, MAYER Annamária, NYAKAS Levente, POGÁCSÁS Anett: A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban. *Iustum Aequum Salutare*, VII. 2011/4. 83.
[796] Lottie LANE: Artificial Intelligence and Human Rights: Corporate Responsibility in AI Governance Initiatives. *Nordic Journal of Human Rights*, vol. 41., issue 4. (2023), 309.

kockázatalapú megközelítése az adatvédelmi gyakorlatba is „átragadhat”. Mivel a GDPR-t az elmúlt években jelentős kritikák érték a szabályok megszorító értelmezéséből következő elvesztegetett gazdasági lehetőségek, fejlődési potenciál miatt,[797] így ezen félelmeket adott esetben tompíthatja egy még inkább piac-szempontú jogalkalmazási gyakorlat. Sőt, adott esetben még az európai mintára „újjászülető” amerikai szabályozási környezet is lehetőséget biztosíthat az alapvető adatvédelmi követelmények technológiai környezetben való újra értelmezéséhez.

9. Irodalomjegyzék

Folyóiratokban megjelent tanulmányok:

- Adam J. Andreotta, Nin Kirkham, Marco Rizzi: AI, big data, and the future of consent. AI & Society. vol. 37. (2022), https://doi.org/10.1007/s00146-021-01262-5.
- Alan Mathison Turing: Computing Machinery and Intelligence. Mind, vol. 59., no. 236. (October 1950)
- Angela Huyue Zhang: The Promise and Perils of China's Regulation of Artificial Intelligence, University of Hong Kong Faculty of Law Research Paper No. 2024/02. (January 28, 2024), https://ssrn.com/abstract=4708676, http://dx.doi.org/10.2139/ssrn.4708676
- Anupam Chander, Margot E. Kaminski, William McGeveran: Catalyzing Privacy Law. Minnesota Law Review, 105 (2021).
- Balogh Zsolt György, Kiss Attila, Polyák Gábor, Szádeczky Tamás, Szőke Gergely László: Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén. Pro Futuro, 2014/1. https://doi.org/10.26521/Profuturo/2014/1/5494. 41.
- Boris Lubarsky: Re-Identification of „Anonymized” Data. Georgetown Law Technology Review, 1. (2017)
- Bryce Goodman, Seth Flaxman: European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine*, vol. 38., no. 3. (2017), https://arxiv.org/abs/1606.08813v3, https://doi.org/10.48550/arXiv.1606.08813
- Carina Dorneck, Ulrich M. Gassner, Jens Kersten, Josef Franz Lindner, Kim Philip Linoh, Katja Nebe, Henning Rosenau, Birgit Schmidt am Busch: Contextual Consent

[797] THOUVENIN op. cit. 254.

– Selbstbestimmung diesseits der Illusionen des Medizinrechts, Medizinrecht, 2019/37. https://doi.org/10.1007/s00350-019-5247-2

- Carlos I. Gutierrez, Anthony Aguirre, Risto Uuk, Claire C. Boine, Matija Franklin: A Proposal for a Definition of General Purpose Artificial Intelligence Systems. Digital Society, 2/36. (2023).
- Chronowski Nóra, Kálmán Kinga, Szentgáli-Tóth Boldizsár: Régi keretek, új kihívások: a mesterséges intelligencia prudens bevonása a bírósági munkába és ennek hatása a tisztességes eljáráshoz való jogra. Glossa Iuridica, VIII/4. 2022.
- Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, Luciano Floridi: Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. 2024.01.17, last revised: 2024.03.15.), arXiv:2401.07348v4, https://doi.org/10.48550/arXiv.2401.07348
- Czapári Dóra, Szőke Gergely László: Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása. JURA, 2022/4.
- Daniel Necz: Data Segregation and its Privacy Aspects. Iustum Aequum Salutare, XIX/2023. 3.
- Darázs Lénárd: Innováció üzleti titok és know-how hasznosítás útján. Magyar Tudomány, 2022/9.
- Deepa Ravindranath: A Guide to Commercial Innovation in Artificial Intelligence. Les Nouvelles - Journal of the Licensing Executives Society, vol. 52. no. 4. (September 2017), https://ssrn.com/abstract=3009423
- Eszteri Dániel: Elosztott mesterséges intelligencia fejlesztés blokklánc alapon az adatvédelem érvényesülése érdekében. Pro Futuro, 2020/1, https://doi.org/10.26521/Profuturo/2020/1/7554.
- Firniksz Judit: Az interoperabilitásra vonatkozó elvárások a digitális piacok szabályozási kontextusában. In Medias Res, 2023/2.
- Florent Thouvenin: Informational Self-Determination: A Convincing Rationale for Data Protection Law?. JIPITEC, 12/2021
- Francesco Ciclosi, Fabio Massacci: "The Data Protection Officer: A Ubiquitous Role That No One Really Knows". IEEE Security & Privacy, vol. 21, no. 01. (2023). doi: 10.1109/MSEC.2022.3222115

- Gintaré Surblyté: Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy. *GRUR International*, vol. 65., issue 12. (2016).
- Gosztonyi Gergely: A kínai internetcenzúra modellje. Pro Futuro, 2022/1, https://doi.org/10.26521/profuturo/2022/1/11118
- Hannah Brown, Katherine LEE, Fatemehsadat MIRESHGHALLAH, Reza SHOKRI, Florian Tramèr: What Does it Mean for a Language Model to Preserve Privacy?. Szöul (2022. június 21-24.): *ACM Conference on Fairness, Accountability, and Transparency (FAccT '22). ACM*, New York, USA, June 2022, https://doi.org/10.1145/3531146.3534642
- Heike Felzmann, Eduard Fosch Villaronga, Christoph Lutz, Aurelia Tamò Larrieux: Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society 6/1. (June 2019). https://doi.org/10.1177/2053951719860542. 10.1177/2053951719860542
- Heleen Janssen, Michelle Seng Ah Lee, Jatinder Singh: Practical fundamental rights impact assessments, International Journal of Law and Information Technology, vol. 30, issue 2. (Summer 2022), https://doi.org/10.1093/ijlit/eaac018
- Herke Csongor: Deepfake: áldás vagy átok? Jogi szabályozási szempontok. Pro Futuro, 2023/13. 1. https://doi.org/10.26521/profuturo/2023/1/13334
- Hideyuki Matsumi, Daniel J. Solove: The Prediction Society: AI and the Problems of Forecasting the Future. GWU Law School Public Law Research Paper No. 2023-58. (2024). https://ssrn.com/abstract=4453869, http://dx.doi.org/10.2139/ssrn.4453869
- Isaac Asimov: Runaround. Astounding Science-Fiction, 1942, 29(1)
- Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, Karen Melham: Dynamic consent: a patient interface for twenty-first century research networks. European Journal of Human Genetics, 2015. https://doi.org/10.1038/ejhg.2014.71
- Jason Haas: Deepfake dilemma. Intellectual property magazine, 2044-7175. (September 2019)
- Jevan Hutson, Ben Winters: America's Next 'Stop Model!': Model Deletion. Georgetown Law Technology Review, vol. 8. no. 1. (January 2024)
- John R. Searle: Minds, brains, and programs. Behavioral and Brain Sciences, vol. 3., issue 3. (September 1980). doi:10.1017/S0140525X00005756.

- Josephine Wolff, William Lehr, Christopher S. Yoo: Lessons from GDPR for AI Policymaking. Virginia Journal of Law & Technology, vol. 27. no. 4. (2024)
- Kai Packhäuser, Sebastian Gündel, Nicolas Münster, Christopher Syben, Vincent Christlein, Andreas Maier: Deep learning-based patient re-identification is able to exploit the biometric nature of medical chest X-ray data. Scientific Reports, 12. 14851 (2022). https://doi.org/10.1038/s41598-022-19045-3
- Karl Manheim, Lyric Kaplan: Artificial Intelligence: Risks to Privacy and Democracy. Yale Journal of Law & Technology, vol. 21., no. 106. (2019)
- Kirk J. Nahra: The Past, Present, and Future of U.S. Privacy Law. Seton Hall Law Review, vol. 51., issue 5 (2021)
- Kis Kelemen Bence, Hohman Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. Infokommunikáció és jog, 2016/2.
- Kiss Attila: A közterületi térfigyelő rendszerek szabályozásának kihívásai a magyar jogalkotásban és a jogalkalmazásban. Infokommunikáció és jog, 2011/4.
- Koltay András, Mayer Annamária, Nyakas Levente, Pogácsás Anett: A médiaszolgáltatás és a sajtótermék fogalma az új magyar médiaszabályozásban. Iustum Aequum Salutare, VII. 2011/4.
- Koltay András: A social media platformok jogi státusa a szólásszabadság szempontjából. In Medias Res, 2019/1. 25.
- Koltay András: A véleményszabadság alkotmányos védelme az Alaptörvény első évtizedében. Acta Humana, 2021/2.
- Liane Colonna: Exploring the Relationship between Article 22 of the General Data Protection Regulation and Article 14 of the Proposed AI Act. Faculty of Law, Stockholm University Research Paper No. 124, 2024.02.16, https://ssrn.com/abstract=4729206, http://dx.doi.org/10.2139/ssrn.4729206
- Lottie Lane: Clarifying Human Rights Standards Through Artificial Intelligence Initiatives. International and Comparative Law Quarterly, vol. 71., issue 4. (2022)
- Lottie Lane: Artificial Intelligence and Human Rights: Corporate Responsibility in AI Governance Initiatives. Nordic Journal of Human Rights, vol. 41., issue 4. (2023)
- Luc Rocher, Julien M. Hendrickx, Yves-Alexandre de Montjoye: Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, 10. 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3

- Marketa Trimble: Artificial Intelligence and Human Intelligence. GRUR International, vol. 72., issue 1. (January 2023), https://doi.org/10.1093/grurint/ikac109
- Mark Owen, Maria Luchian: Following the AI path. Intellectual property magazine, 2044-7175. (September 2020).
- Mezei Kitti: A mesterséges intelligencia jogi szabályozásának aktuális kérdései az Európai Unióban. In Medias Res, 2023/01. https://doi.org/10.59851/imr.12.1.4. 62
- Michèle Finck, Frank Pallas: They who must not be identified—distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, vol. 10., issue 1. (2020).
- Mirko Forti: The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR. European Journal of Legal Studies 13 (1). (2021), https://ssrn.com/abstract=3866576
- Nadezhda Purtova: The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, vol. 10., issue 1. (2018). https://doi.org/10.1080/17579961.2018.1452176.
- Necz Dániel: A mesterséges intelligencia hatása a szerzői jogra. Iparjogvédelmi és Szerzői Jogi Szemle, 2018/12.
- Necz Dániel: A mesterséges intelligencia belügyi és biztonsági célú alkalmazása. Scientia et Securitas, 2020/1. 1.
- Necz Dániel: A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. Rendvédelem, 2020/01.
- Necz Dániel: A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai. Acta Humana – Emberi Jogi Közlemények, 2022/3. https://doi.org/10.32566/ah.2022.3.4
- Nello Cristianini, Teresa Scantamburlo: On social machines for algorithmic regulation, AI & Society, 2020/35, https://doi.org/10.1007/s00146-019-00917-8
- Omer Tene: Privacy: The new generations. International Data Privacy Law, vol. 1., issue 1. (2011)
- Omer Tene, Jules Polonetsky: A Theory of Creepy: Technology, Privacy and Shifting Social Norms. Yale Journal of Law & Technology, vol. 16., no. 59. (2013)
- Omer Tene, Jules Polonetsky: Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property, vol. 11., issue 5. (2013)

- Palkó Tamás: A mesterséges intelligencia kutatása az Európai Unióban. Európai Jog, 20/4, 2020. 21.
- Paul Jurcys, Chris Donewald, Jure Globocnik, Markus Lampinen: My Data, My Terms: A Proposal for Personal Data Use Licenses. Harvard Journal of Law & Technology, vol. 33., Digest Spring 2020, https://jolt.law.harvard.edu/assets/digestImages/Paulius-Data-licenses-HJOLTDigest-Feb20.pdf
- Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, vol. 57. (2010), https://ssrn.com/abstract=1450006
- Philip Hacker, Andreas Engel, Marco Mauer: Regulating ChatGPT and other Large Generative AI Models. FAccT '23 Chicago (2023.06.12-15). arXiv:2302.02337v8, https://doi.org/10.48550/arXiv.2302.02337
- Raphaël Gellert: Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. International Data Privacy Law, vol. 11., issue 2. (2021)
- Samuel D. Warren – Louis D. Brandeis: The Right to Privacy. Harvard Law Review, vol. 4., no. 5. (1890)
- Sandra Wachter, Brent Mittelstadt: A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. Columbia Business Law Review, 2019(2).
- Sandra Wachter, Brent Mittelstadt, Luciano Floridi: Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, vol. 7., issue 2. (2017)
- Schubauer Petra: Az elfeledtetéshez való jog az új Adatvédelmi Rendelet tükrében. Infokommunikáció és jog, 2017/2.
- Shlomit Yanisky-Ravid, Sean Hallisey: 'Equality and Privacy by Design': Ensuring Artificial Intelligence (AI) Is Properly Trained & Fed: A New Model of AI Data Transparency & Certification As Safe Harbor Procedures, 2018.11.05, https://ssrn.com/abstract=3278490, http://dx.doi.org/10.2139/ssrn.3278490
- Szabó Endre: Az adatvédelmi tisztviselőről. A GDPR szabályainak elemzése. Infokommunikáció és jog, 2018/1. 7.

- Szabó Hedvig: A mesterséges intelligenciára vonatkozó szabályozás, jogalkotás a rendvédelem tükrében. MTA Law Working Papers, 2023/16, https://jog.tk.hu/mtalwp/a-mesterseges-intelligenciara-vonatkozo-szabalyozas-jogalkotas-a-rendvedelem-tukreben?download=pdf
- Szegedi László, Dornfeld László, Polgár Zoltán, Teleki Bálint: A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – egységes szabályozás, eltérő alkalmazás?. Infokommunikáció és jog, 2021/1.
- Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és jog, 2013/3.
- Tae Wan Kim, Bryan R. Routledge: Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach. Business Ethics Quarterly, vol. 32., no. 1 (2022). doi:10.1017/beq.2021.3
- Thomas Davenport, Ravi Kalakota: The potential for artificial intelligence in healthcare. Future Healthcare Journal, 2019 Jun;6(2):94-98. doi: 10.7861/futurehosp.6-2-94. PMID: 31363513; PMCID: PMC6616181.
- Tóth András: Az online platformok európai szabályozása. In Medias Res, 2022/2. 79.
- Török Bernát: Közösségi média – társadalmi párbeszéd. Fundamentum, 2022/3.
- Udvary Sándor: Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései. Gazdaság és jog, 2018/12.
- Yilun Wang, Michael Kosinski: Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, vol. 114, issue 2. (2018). https://doi.org/10.1037/pspa0000098
- Yves-Alexandre de MONTJOYE, César A. HIDALGO, Michel VERLEYSEN, Vincent D. BLONDEL: Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports, 3. 1376 (2013). https://doi.org/10.1038/srep01376
- William L. Prosser: Privacy. California Law Review, vol. 48., no. 3. (1960)
- Wolfgang Kerber: Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. GRUR International, vol. 72., issue 2. (2023)
- Ződi Zsolt: Privacy és a Big Data. Fundamentum, 2017/1-2.
- Ződi Zsolt: Az európai platformszabályozás jellegzetességei. Platformjog és felhasználóvédelem. In Medias Res, 2022/1.

Monográfiák, könyvfejezetek:

- Andrea Pin: Artificial Intelligence, the Public Space, and the Right to be Ignored. In: Alberto Quintavalla, Jeroen Temperman (eds.): Artificial Intelligence and Human Rights. Oxford University Press, 2023.
- Bakos-Kovács Kitti: Magánélet a hálózat csapdájában – a „személyiségprofilok" jogi értékelése. In: Görög Márta, Menyhárd Attila, Koltay András (szerk.): A személyiség védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017.
- Böcskei Balázs, Német Szilvi: Toxikus technokultúrák és digitális politika. Érzelmek, mémek, adatpolitika és figyelem az interneten. Budapest, Napvilág Kiadó – TK PTI, 2021.
- Brian Christian: The Most Human Human. New York, Anchor Books, 2011.
- Buzás Péter: Az érintett jogai. In: Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary Kft., 2021, második, átdolgozott kiadás
- Christoph Bartneck, Christoph Lütge, Alan Wagner, Sean Welsh: An Introduction to Ethics in Robotics and AI. Cham, Springer, 2021, eBook. https://doi.org/10.1007/978-3-030-51110-4. 68.
- Chris Reed: Data Trusts for Lawful AI Data Sharing. In: Gary Chan Kok Yew, Man Yip (eds.): AI, Data and Private Law, Translating Theory into Practice, Hart Publishing, 2021.
- Clarisse Laupman, Laurianne-Marie Schippers, Marilia Papaléo Gagliardi: Biased Algorithms and the Discrimination upon Immigration Policy. In: Bart Custers, Eduard Fosch-Villaronga: Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice, The Hague, T.M.C. Asser Press, 2022.
- Freidler Gábor: A személyes adatok védelméhez való jog jelentése. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve. Budapest, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., 2008.
- Eduard Fosch-Villaronga: Robots, Healthcare, and the Law. Regulating Automation in Personal Care, e-book version, 2020.
- Elek István: Az intelligencia spontán megjelenése. Budapest, ELTE Eötvös Kiadó, 2015.

- Eszteri Dániel: A deepfake-technológia adatvédelmi értékelése a GDPR tükrében. In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Gondolat Kiadó, 2023.
- Felipe Romero Moreno: Generative AI and deepfakes: a human rights approach to tackling harmful content. International Review of Law, Computers & Technology, 2024. https://doi.org/10.1080/13600869.2024.2324540
- Hajdú József: A mesterséges intelligencia hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját. Infokommunikáció és jog, 2020/2.
- Hannah Fry: Emberek és gépek. Hogyan tartsuk a kezünkben az irányítást a mesterséges intelligencia korában? Budapest, HVG Kiadó Zrt, 2021. Fordította: Dembinszky Zsófia (2020), eredeti kiadás: 2018.
- Hubert L. Dreyfus: What Computers Still Can't Do. A Critical of Artificial Reason. Cambridge, London, The MIT Press, 1992.
- Jacob Livingston Slosser: Artificial Intelligence and Public Law. In: Mariana Valverde, Kamari M. Clarke, Eve Darian Smith, Prabha Kotiswaran (eds.): The Routledge Handbook of Law and Society. London, Routledge, 2021.
- Joanna J. Bryson: Robots Should Be Slaves. In Yorick Wilks (ed.): Close engagements with artificial companions: key social, psychological, ethical and design issues. John Benjamins Publishing Company. https://doi.org/10.1075/nlp.8.11bry
- Kate Crawford: Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven, London, Yale University Press, 2021.
- Keserű Barna Arnold: A 21. századi technológiai változások hatása a jogalkotásra. Képes-e lépést tartani a jog a változó világgal?, Budapest, Dialóg Campus Kiadó, 2020.
- Kiss Attila: Információbiztonság és adatvédelem. Kapcsolódási pontok a hatályos és az EU adatvédelmi rendelete utáni szabályozásban. In: Czékmann Zsolt (szerk.): Infokommunikációs jog. Budapest, Dialóg Campus Kiadó, 2019.
- Koltay András: Az internetes kapuőrök mint szerkesztők – a kommentek kérdése. In: Görög Márta, Menyhárd Attila, Koltay András (szerk.): A személyiség védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017.
- Koltay András: Freedom of Speech. The Unreachable Mirage. Budapest, Complex Publisher Ltd., 2013.

- Koltay András, Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása, Wolters Kluwer Hungary Kft., Budapest, 2019.
- Komanovics Adrienne: Információszabadság az Európai Unióban, Budapest-Pécs, Dialóg Campus Kiadó, 2009.
- Klein Tamás: Robotok a beteggondozásban és a gyógyításban. In: Klein Tamás, Tóth András (szerk.): Technológia jog – Robotjog – Cyberjog. Budapest, Wolters Kluwer Hungary, 2018.
- Lilian Edwards, Edina Harbinja: 'Be Right Back': What Rights Do We Have over Post-mortem Avatars of Ourselves? In: Lilian Edwards, Burkhard Schafer, Edina Harbinja (eds.): Future Law: Emerging Technology, Regulation and Ethics. Edinburgh, Edinburgh University Press, 2020.
- Menyhárd Attila: A magánélet védelme az Emberi Jogi Bíróság gyakorlatában. In: Görög Márta, Menyhárd Attila, Koltay András: A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017.
- Miskolczi Barna, Szathmáry Zoltán: Büntetőjogi kérdések az információk korában – mesterséges intelligencia, big data, profilozás. Budapest, HVG-Orac Lap- és Könyvkiadó Kft., 2018.
- Paolo Guarda: „Free data?": open science in the age of personal data protection. In: Jacob H. Rooksby (ed.): Research Handbook on Intellectual Property and Technology Transfer. Cheltenham, Northampton, Edmund Elgar Publishing, 2020.
- Papp János Tamás: A rendőrök képmáshoz való jogának kérdése. In: Görög Márta, Menyhárd Attila, Koltay András: A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017.
- Péterfalvi Attila: Algoritmusok és adatvédelem: Quo vadis? A 2020.02.27-i mesterséges intelligencia alkalmazásának hatása az alapjogokra című konferencián elhangzott előadás szerkesztett leirata. In: Török Bernát, Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről. Budapest, Ludovika Egyetemi Kiadó, 2021.
- Péterfalvi Attila, Osztopáni Krisztián: A személyes adatok magánjogi védelme a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlatában. In: Görög Márta, Menyhárd Attila, Koltay András: A személyiség és védelme. Az Alaptörvény

VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Karának dékánja, 2017.

- Pók László Gábor: Védeni vagy megosztani? – A személyes adatok szerepe az internetes platformok szabályozásában. In: Török Bernát, Ződi Zsolt (szerk.): Az internetes platformok kora. Budapest, Ludovika Egyetemi Kiadó, 2022.
- Pusztahelyi Réka: A személyes adatok üzleti célú megszerzésére alkalmazott „sötét minták" elleni fellépés lehetséges formái. In Medias Res, 2023/2.
- Révész Balázs, Az adatkezelés alapelvei. In: Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary Kft., 2021.
- Ron Dolin: Technology Issues in Legal Philosophy. In: Daniel Martin Katz, Ron Dolin, Michael J. Bommarito (eds.): Legal Informatics. Cambridge, New York, Cambridge University Press, 2021.
- Sonja Zillner, Jon Ander GOMEZ, Ana García Robles, Thomas Hahn, Laure Le Bars, Milan Petkovic, Edward Curry: Data Economy 2.0: From Big Data Value to AI Value and a European Data Space. In: Edward Curry, Andreas Metzger, Sonja Zillner, Jean-Christophe Pazzaglia, Ana García Robles (eds.): The Elements of Big Data Value. Foundations of the Research and Innovation Ecosystem. Cham, Springer, https://doi.org/10.1007/978-3-030-68176-0_16
- Tóth András: A web 2.0 versenyjogi vonatkozásai: In: Klein Tamás (szerk.): Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről. Médiatudomány Intézet, 2018.
- Tóth András: Az ingyenesség állítása mint fogyasztóvédelmi kihívás a digitális gazdaságban. In: Rigó Csaba Balázs, Szoboszlai Izabella, Csirszki Martin Milán (szerk.): A hazai fogyasztóvédelmi jog áttekintése: alapok, kihívások, aktualitások. Budapest, Gazdasági Versenyhivatal, 2023.
- Veszelszki Ágnes: Deepfake: kételkedés a kételyben. In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Gondolat Kiadó, 2023.

Internetes hivatkozások:

<u>Önálló tanulmányok, blog cikkek:</u>

- Alessandro Achille, Michael Kearns, Carson Klingenberg, Stefano Soatto: AI Model Disgorgement: Methods and Choices, 2023.04.07, arXiv:2304.03545v1, https://doi.org/10.48550/arXiv.2304.03545
- Alex Shashkevich: Stanford researcher examines earliest concepts of artificial intelligence, robots in ancient myths. Stanford News, 2019.02.28. https://news.stanford.edu/2019/02/28/ancient-myths-reveal-early-fantasies-artificial-life/
- Ayse Gizem Yasar, Andrew Chong, Evan Dong, Thomas Krendl Gilbert, Sarah Hladikova, Roland Maio, Carlos Mougan, Xudong Shen, Shubham Singh, Ana-Andreea Stoica, Savannah Thais, Miri Zilka: AI and the EU Digital Markets Act: Addressing the Risks of Bigness in Generative AI, arXiv:2308.02033, https://doi.org/10.48550/arXiv.2308.02033.
- Blagoj Delipetrev, Chrisa Tsinaraki, Uroš Kostić: AI Watch. Historical Evolution of Artificial Intelligence. Analysis of the three main paradigm shifts in AI. Luxembourg, Publications Office of the European Union, 2020, doi:10.2760/801580.
- Cynthia DWORK: Differential Privacy. Velence (2006. július 10-14.): *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)* | July 2006, Sprinter Verlag, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/dwork.pdf
- Daniel G. BOBROW: Natural Language Input for a Computer Problem Solving System. Cambridge, Massachusetts Institute of Technology, 1964.03.30, https://dspace.mit.edu/bitstream/handle/1721.1/5922/AIM-066.pdf?sequence=2&isAllowed=y
- Domokos Márton, Horváth Anna Zsófia: Dark patterns – napvilágra kerülő sötét megoldások. Jogi Fórum, 2021.09.02. https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/
- Eli MacKinnon, Dr. Jennifer King: Regulating AI Through Data Privacy. Stanford University, Ethics and Justice, Law, Regulation, and Policy, 2022.01.11, https://hai.stanford.edu/news/regulating-ai-through-data-privacy
- John McCarthy: What is Artificial Intelligence? Basic Questions. 2007.11.12. http://www-formal.stanford.edu/jmc/whatisai/node1.html

- Josh A. Goldstein, Girish Sastry, Micah Musser, Renée DiResta, Matthew Gentzel, Katerina Sedova: Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations, January 2023, arXiv:2301.04246
- Katherine Miller: Can't Unsubscribe? Blame Dark Patterns. Stanford University, Human-Centered Artificial Intelligence, 2021.12.13, https://hai.stanford.edu/news/cant-unsubscribe-blame-dark-patterns
- Kristian Lum, Rumman Chowdhury: What is an "algorithm"? It depends whom you ask. MIT Technology Review, 2021.02.26. https://www.technologyreview.com/2021/02/26/1020007/what-is-an-algorithm/
- Larry Hardesty: Explained: Neural networks. MIT News, 2017.04.14. https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414
- Marc Rotenberg: „Privacy in the Modern Age: The Search for Solutions". Marrakech (2016.10.19.): 38th International Conference of the Data Protection and Privacy Commissioners. Elérhető: https://archive.epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf
- Necz Dániel, Az adatkezelésről való tájékoztatás technológiai környezetben, különös tekintettel az Egyesült Államok szabályozására, Jogi Fórum, 2022.08.31. https://www.jogiforum.hu/wp-content/uploads/2022/09/necz-daniel_adatkezelesrol-valo-tajekoztatas-technologiai-kornyezetben_cimlappal.pdf
- Pók László: Mesterséges intelligencia, személyes adatok és az adatkezelés jogalapjai. GDPR Blog, 2023.11.30, https://gdpr.blog.hu/2023/11/30/mesterseges_intelligencia_szemelyes_adatok_es_az_adatkezeles_jogalapjai
- Rockwell ANYOHA: The History of Artificial Intelligence, Harvard SITN Blog, 2017.08.28. http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/
- Ződi Zsolt: Fából vaskarika? Alapjogi hatásvizsgálat a Mesterséges Intelligencia Rendeletben, 2024.03.08, https://www.ludovika.hu/blogok/itkiblog/2024/03/08/fabol-vaskarika/
- Ződi Zsolt: A generatív mesterséges intelligencia szabályozása az MI rendeletben, 2024.04.29, https://www.ludovika.hu/blogok/itkiblog/2024/04/29/a-generativ-mesterseges-intelligencia-szabalyozasa-az-mi-rendeletben/

Egyéb internetes hivatkozások:

- Alice chatbot wins for third time. BBC News, last updated: 2004.09.20. http://news.bbc.co.uk/2/hi/technology/3672424.stm
- AMA, Advancing health care AI through ethics, evidence and equity, https://www.ama-assn.org/practice-management/digital/advancing-health-care-ai-through-ethics-evidence-and-equity
- AMA, Augmented intelligence in healthcare, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf
- Annie Brown: Understanding The Technical And Societal Relationship Between Shadowbanning And Algorithmic Bias. Forbes, 2021.10.27, https://www.forbes.com/sites/anniebrown/2021/10/27/understanding-the-technical-and-societal-relationship-between-shadowbanning-and-algorithmic-bias/
- AWS, What's the difference between AI and Machine Learning?, https://aws.amazon.com/compare/the-difference-between-artificial-intelligence-and-machine-learning/
- Benjamin Weiser, Nate Schweber: The ChatGPT Lawyer Explains Himself, New York Times, 2023.06.08, https://www.nytimes.com/2023/06/08/nyregion/lawyer-chatgpt-sanctions.html
- Brandon Lalonde: Explaining model disgorgement. IAPP, 2023.12.13, https://iapp.org/news/a/explaining-model-disgorgement/
- Byron Kaye: Australian mayor readies world's first defamation lawsuit over ChatGPT content. Reuters, 2023.04.05, https://www.reuters.com/technology/australian-mayor-readies-worlds-first-defamation-lawsuit-over-chatgpt-content-2023-04-05/
- ChatGPT, https://openai.com/blog/chatgpt
- Dario Casella, Laurence Lawson: AI and privacy: Everything you need to know about trust and technology. Ericsson, 2022.08.01. https://www.ericsson.com/en/blog/2022/8/ai-and-privacy-everything-you-need-to-know
- Dylan Love: It Gets Pretty Weird When You Have Two 'Artificially Intelligent' Chatbots Talk To Each Other. Insider, 2014.05.31. https://www.businessinsider.com/artificial-intelligence-chatbots-and-the-turing-test-2014-5?r=US&IR=T.
- Edith M. Lederer: UN council to hold first meeting on potential threats of artificial intelligence to global peace. AP News, 2023.07.03,

https://apnews.com/article/artificial-intelligence-un-security-council-meeting-uk-f7fb6d8f8a261a9d9b23ca463ee29d3d

- Electronic Privacy Information Center, The State of State AI Laws: 2023, 2023.08.03., https://epic.org/the-state-of-state-ai-laws-2023/
- ELIZA: a very basic Rogerian psychoterapist chatbot. https://web.njit.edu/~ronkowit/eliza.html
- Emily Flitter, Stacy Cowley, Voice Deepfakes Are Coming for Your Bank Balance, New York Times, 2023.08.30., https://www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html
- European Commission, AI Pact, https://digital-strategy.ec.europa.eu/en/policies/ai-pact
- European Commission, Commission appoints expert group on AI and launches the European AI Alliance, DIGIBYTE, European Commission, 2018.06.14, https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance
- European Commission, Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act, 30 April 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373
- European Commission, Launch of the European Blockchain Regulatory Sandbox, 2023.02.14, https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox
- European Council, Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world, 2023.12.09, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/
- European Council, Press release, Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights, 2022.12.06, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/
- Explainable AI, Google, https://cloud.google.com/explainable-ai
- Facebook-hírfolyamban megjelenő tartalmak beállítása, https://www.facebook.com/help/1913802218945435

- Future of Life Institute, Pause Giant AI Experiments: An Open Letter, https://futureoflife.org/open-letter/pause-giant-ai-experiments/
- GPAI, https://gpai.ai/about/
- Google Ads Súgó, Aukció, https://support.google.com/google-ads/answer/142918?hl=hu
- Google AI, Our Principles, https://ai.google/responsibility/principles/
- Google, Bard Experiment, https://bard.google.com/?hl=en
- Google. Gemini Apps Privacy Hub, https://support.google.com/gemini/answer/13594961?hl=en#collected_data&zippy=%2Cwhy-does-google-retain-my-conversations-after-i-turn-off-gemini-apps-activity-and-what-does-google-do-with-this-data
- Google, Perspectives on Issues in AI Governance, https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf
- Google, Recommendations for Regulating AI, https://ai.google/static/documents/recommendations-for-regulating-ai.pdf
- Hannah Roberts: Is The Rise in AI Use Damaging Junior Lawyers' Skills. Law.com International, 2020.07.13, https://www.law.com/international-edition/2020/07/13/is-the-rise-in-ai-use-damaging-junior-lawyers-skills/?slreturn=20230725124725
- Henry Bodkin: Microdrones: the AI assassins set to become weapons of mass destruction. The Telegraph, 2022.11.14. https://www.telegraph.co.uk/global-health/terror-and-security/drone-assassins-micro-killing-machine/
- IAB Europe, TCF – Transparency & Consent Framework, https://iabeurope.eu/transparency-consent-framework/
- IAPP. Vimeo settles biometric privacy lawsuit; Tesla faces privacy class action, 2023.04.11, https://iapp.org/news/a/vimeo-settles-biometric-privacy-lawsuit-tesla-faces-privacy-class-action/
- IBM, AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?. https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/
- Tim Mucci: Five open-source AI tools to know, 2023.12.15, https://www.ibm.com/blog/five-open-source-ai-tools-to-know/
- IBM, Red teaming 101: What is red teaming?, https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/

- IBM, Strong AI vs. weak AI. https://www.ibm.com/topics/strong-ai
- IBM, watsonx.governance, https://www.ibm.com/products/watsonx-governance
- Kashmir Hill: How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Forbes, 2012.02.16, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/
- Ken Macdonald: Police to use AI recognition drones to help find the missing. BBC News, Scotland, 2019.11.04. https://www.bbc.com/news/uk-scotland-50262650
- Lance Eliot: Generative AI ChatGPT Can Disturbingly Gobble Up Your Private And Confidential Data, Forewarns AI Ethics And AI Law, Forbes, 2023.01.27. https://www.forbes.com/sites/lanceeliot/2023/01/27/generative-ai-chatgpt-can-disturbingly-gobble-up-your-private-and-confidential-data-forewarns-ai-ethics-and-ai-law/
- Lego, Now some serious stuff, https://www.lego.com/en-us/kids/legal/privacy-policy-short
- Matt Sheehan: China's AI Regulations and How They Get Made, July 2023, Carnegie Endowment for International Peace, https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf
- Meredith Somers: Deepfakes, explained, MIT Management Sloan School, Ideas Made to Matter, 2020.07.21, https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained
- Meta AI, Facebook's five pillars of Responsible AI, 2021.06.22, https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/
- Meta, Good Questions, Real Answers: How Does Facebook Use Machine Learning to Deliver Ads?, 2020.06.11, https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads
- Meta, Privacy progress update, We have a responsibility to protect people's privacy and give them control to make their own choices, https://about.meta.com/privacy-progress?utm_source=about.facebook.com&utm_medium=redirect
- Michelle Toh, Yoonjung Seo: OpenAI CEO calls for global cooperation to regulate AI. CNN Business, 2023.06.09. https://edition.cnn.com/2023/06/09/tech/korea-altman-chatgpt-ai-regulation-intl-hnk/index.html

- Microsoft, Democratizing AI: Satya Nadella on AI vision and societal impact at DLD, 2017.01.17, https://news.microsoft.com/europe/2017/01/17/democratizing-ai-satya-nadella-shares-vision-at-dld/
- Microsoft, Putting principles into Practice: How we approach responsible AI at Microsoft, https://www.microsoft.com/cms/api/am/binary/RE4pKH5#:~:text=At%20Microsoft%2C%20we've%20recognized,inclusiveness%2C%20transparency%2C%20and%20accountability
- Midjourney, https://www.midjourney.com/
- Midjourney, Privacy Policy, https://docs.midjourney.com/docs/privacy-policy
- Mistral AI, https://mistral.ai/
- National Artificial Intelligence Initiative, https://www.ai.gov/
- National Cybersecurity Center of Excellence, Artificial Intelligence: Adversarial Machine Learning, https://www.nccoe.nist.gov/ai/adversarial-machine-learning
- National Cyber Security Center, Guidelines for secure AI system development, https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
- Network Working Group, V. Cerf, PARRY Encounters the DOCTOR, 1973.01.21. https://datatracker.ietf.org/doc/html/rfc439
- Nicole Kobie: The complicated truth about China's social credit system. Wired, 2019.06.07. https://www.wired.co.uk/article/china-social-credit-system-explained
- NIST, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework
- OpenAI, How your data is used to improve model performance, https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance
- OpenAI. Sora, https://openai.com/sora
- Open Future, Defining best practices for opting out of ML trainings, https://openfuture.eu/wpcontent/uploads/2023/09/Best_practices_for_optout_ML_training.pdf
- PlexTrac, What Is Purple Teaming?, https://plextrac.com/what-is-purple-teaming/
- Politico, Open Letter to the European Commission, Artificial Intelligence and Robotics, https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf.

- Rem Darbinyan: How AI Transforms Social Media. Forbes, 2023.03.16, https://www.forbes.com/sites/forbestechcouncil/2023/03/16/how-ai-transforms-social-media/
- Reuters, Elon Musk's Neuralink implants brain chip in first human, 2024.01.30, https://www.reuters.com/technology/neuralink-implants-brain-chip-first-human-musk-says-2024-01-29/
- Rory Cellan-Jones: Stephen Hawking warns artificial intelligence could end mankind. BBC News, 2014.12.02, https://www.bbc.com/news/technology-30290540
- Siobhan Roberts: Christopher Strachey's Nineteen-Fifties Love Machine, New Yorker, 2017.02.14. https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine
- Tom Clarke: Artificial intelligence 'doesn't have capability to take over', Microsoft boss says. Sky News, 2023.07.07, https://news.sky.com/story/artificial-intelligence-doesnt-have-capability-to-take-over-microsoft-boss-says-12916709
- Tom Simonite: Now That Machines Can Learn, Can They Unlearn?, Wired, 2021.08.19, https://www.wired.com/story/machines-can-learn-can-they-unlearn/
- Worker Info Exchange, Just Beat It! How Just Eat Robo-fires its Workers, April 2023, https://www.workerinfoexchange.org/just-eat-report. 1.
- YouTube Help. Autoplay videos, https://support.google.com/youtube/answer/6327615?hl=en#:~:text=If%20you're%2018%20or,Autoplay%20settings%20for%20different%20devices
- Zach Williams: NY AG Tish James bashes MSG facial surveillance as 'plagued' with legal problems. New York Post, 2023.01.25, https://nypost.com/2023/01/25/ag-letitia-james-demands-docs-from-msg-about-facial-surveillance-of-legal-enemies/

Jogszabályok:

Nemzetközi jogszabályok és egyéb dokumentumok:

- Convention on the Rights of the Child: The child-friendly version, UNICEF https://www.unicef.org/sop/convention-rights-child-child-friendly-version
- Council of Europe, Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law, https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680aee411

- Developing Advanced AI Systems, https://ec.europa.eu/newsroom/dae/redirection/document/99641
- Digital Agency, Data Free Flow with Trust (DFFT), https://www.digital.go.jp/en/dfft-en/
- Európa Tanács, Egyezmény a Mesterséges Intelligenciáról, az Emberi Jogokról, A Demokráciáról és a Jog Uralmáról, https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f
- Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, https://ec.europa.eu/newsroom/dae/redirection/document/99641
- Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI, https://www.mofa.go.jp/files/100573471.pdf
- OECD, AI Principles, https://oecd.ai/en/ai-principles
- OECD, Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, 5 March 2024, https://doi.org/10.1787/623da898-en

Európai uniós jogszabályok és egyéb dokumentumok:

- A Bizottság határozata (2001. december 20.) a 95/46/EK európai parlamenti és tanácsi határozat értelmében a személyes adatoknak a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő védelméről (az értesítés a C(2001) 4539. számú dokumentummal történt), HL L 2., 2002.1.4, p. 13–16 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4, p. 89–131 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

- Jelentés a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi ajánlásokról (2015/2103(INL)), A8-0005/2017, 2017.01.24.
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A közös európai adattér kialakítása felé, Brüsszel, 25.4.2018, COM(2018) 237 final
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A mesterséges intelligenciáról szóló összehangolt terv, Brüsszel, 2018.12.7., COM(2018) 795 végleges
- 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, Brüsszel, 2019.4.8., COM(2019) 168 final
- Az Európai Parlament és a Tanács (EU) 2019/790 irányelve (2019. április 17.) a digitális egységes piacon a szerzői és szomszédos jogokról, valamint a 96/9/EK és a 2001/29/EK irányelv módosításáról, PE/51/2019/REV/1, HL L 130., 17/05/2019, p. 92–125 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, Brüsszel, 2020.2.19. COM(2020) 65 final
- 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, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, Brüsszel, 2021.4.21, COM(2021) 206 final, 2021/0106(COD)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A mesterséges intelligenciával kapcsolatos európai megközelítés előmozdítása, Brüsszel, 2021.4.21. COM(2021) 205 final
- A Bizottság (EU) 2021/1772 végrehajtási határozata (2021. június 28.) az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről (az értesítés a C(2021) 4800. számú dokumentummal történt) (EGT-vonatkozású szöveg), C/2021/4800, HL L 360.,

2021.10.11, p. 1–68 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

- A Bizottság (EU) 2021/1773 végrehajtási határozata (2021. június 28.) az (EU) 2016/680 európai parlamenti és tanácsi irányelv szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről (az értesítés a C(2021) 4801. számú dokumentummal történt), C/2021/4801, HL L 360., 2021.10.11, p. 69–107 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Javaslat, az Európai Parlament és a Tanács irányelve a platformalapú munkavégzés munkakörülményeinek javításáról, Brüsszel, 2021.12.9. COM(2021) 762 final, 2021/0414(COD)
- Az Európai Parlament es a Tanács (EU) 2022/1925 rendelete, a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály), PE/17/2022/REV/1, HL L 265., 2022.10.12, p. 1–66 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (EGT-vonatkozású szöveg), PE/30/2022/REV/1, HL L 277., 2022.10.27, p. 1–102 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Európai Parlament, Jelentés a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról - A9-0188/2023, 2023.05.22, COM(2021)0206
- Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete (2023. december 13.) a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról, valamint az (EU) 2017/2394 rendelet és az (EU) 2020/1828 irányelv módosításáról (adatrendelet), PE/49/2023/REV/1, HL L, 2023/2854, 2023.12.22, ELI: http://data.europa.eu/eli/reg/2023/2854/oj (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Helyesbites az Európai Parlament által 2024. március 13-án a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a

300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet és a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló jogszabály) szóló (EU) 2024/... európai parlamenti és tanácsi rendelet elfogadására tekintettel első olvasatban elfogadott álláspontho z, P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), cor01. 17.4.2024

Amerikai jogszabályok:

- California Consumer Privacy Act of 2018, https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law.
- Executive Order 13859 of February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence
- National Artificial Intelligence Initiative Act of 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210
- Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/6580/text
- Blueprint for an AI Bill of Rights, Making Automated Systems Work for the American People, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf
- AI Foundation Model Transparency Act of 2023, https://beyer.house.gov/uploadedfiles/ai_foundation_model_transparency_act_text_118.pdf
- Artificial Intelligence Research, Innovation, and Accountability Act of 2023, https://www.thune.senate.gov/public/_cache/files/7dea8daa-f6d1-4881-ad21-2381fcbe0785/6362CE1D0A17743166BC170A593B5CDA.ccaskfall23a15.pdf
- The White House. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 2023.10.30, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

- The White House, G7 Leaders' Statement on the Hiroshima AI Process, 2023.10.30, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/
- The White House, G7 Leaders' Statement, 2023.12.06, https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/06/g7-leaders-statement-6/
- American Privacy Rights Act of 2024, https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf
- An Act Preventing a Dystopian Work Environment (H.1873), https://malegislature.gov/Bills/193/H1873
- Artificial Intelligence Video Interview Act, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68
- Assembly Bill No. 331, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=202320240AB331&version=20230AB33195AMD
- Assembly Bill No. 602, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB602
- Assembly Bill No. 730, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201920200AB730&version=20190AB73093CHP, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730
- Ensuring Likeness, Voice and Image Security (ELVIS) Act of 2024, https://legiscan.com/TN/text/HB2091/id/2900923
- Federal Trade Commission, Joint Statement on Enforcement Efforts against Discrimination and Bias in Automated Systems, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf
- House Bill 1063, https://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2023&sind=0&body=H&type=B&bn=1063
- Local Law 144 of 2021 regarding automated employment decision tools, https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page

- New York State Assembly. S01042 Memo, https://nyassembly.gov/leg/?default_fld=%0D%0A&leg_video=&bn=S01042&term=2023&Summary=Y&Actions=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y

Magyar jogszabályok, stratégiai dokumentumok:

- Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény
- A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény
- Innovációs és Technológiai Minisztérium: Magyarország Mesterséges Intelligencia Stratégiája 2020–2030, 2020, https://ai-hungary.com/api/v1/companies/15/files/137203/view
- Innovációs és Technológiai Minisztérium: Magyarország Mesterséges Intelligencia Stratégiája 2020–2030, 2020, https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

További országok jogszabályai és egyéb joganyagok:

- HM Government, Online Harms Whitepaper, 2019. április, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf
- Government of the Netherlands, Impact Assessment Fundamental Rights and Algorithms, 2022.03.31, https://www.government.nl/documents/reports/2022/03/31/impact-assessment-fundamental-rights-and-algorithms
- Department for Science, Innovation & Technology, A pro-innovation approach to AI regulation, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1176103/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf
- The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023, 2023.11.01, https://www.gov.uk/government/publications/ai-safety-

summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

- OECD.AI, Pan-Canadian AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-14828
- Parliament of Canada, BILL C-27, https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading
- Artificial Intelligence (Regulation) Bill [HL], https://bills.parliament.uk/publications/53068/documents/4030

Bírósági gyakorlat:

Az Emberi Jogok Európai Bíróságának gyakorlata:

- Amman v. Switzerland, no. 27798/95., 2000. február 16-i ítélet
- Rotaru v. Romania, no. 28341/95., 2000. május 4-i ítélet
- Axel Springer AG v. Germany, no. 39954/08., 2012. február 7-i ítélet
- Delfi v Estonia, no. 64569/09, 2015. június 16-i ítélet
- Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary, no. 22947/13, 2016. február 2-i ítélet
- Bărbulescu v. Romania, no. 61496/08., 2017. szeptember 5-i ítélet
- Egill Einarsson v. Iceland, no 24703/15, 2017. november 7-i ítélet
- Biancardi v. Italy, no. 77419/16., 2021. november 25-i ítélet
- Hubarlain v. Belgium, no. 57292/16., 2023. július 4-i ítélet

Az Európai Unió Bíróságának gyakorlata:

- C-131/12. sz. ügy Google Spain SL, a Google Inc. és az Agencia Española de Protección de Datos, Mario Costeja González között folyamatban lévő eljárásban [ECLI:EU:C:2014:317]
- C-582/14. sz. ügy Patrick Breyer kontra Bundesrepublik Deutschland [ECLI:EU:C:2016:779]
- C-434/16. sz. ügy Peter Nowak kontra Data Protection Commissioner [ECLI:EU:C:2017:994]
- C-184/20. sz. ügy OT kontra Vyriausioji tarnybinės etikos komisija [ECLI:EU:C:2022:601]

- T-557/20. sz. ügy Egységes Szanálási Testület kontra európai adatvédelmi biztos [ECLI:EU:T:2023:219]
- C-129/21. sz. ügy Proximus NV kontra Gegevensbeschermingsautoriteit [ECLI:EU:C:2022:833]
- C-252/21. sz. ügy Meta Platforms Inc. és társai kontra Bundeskartellamt [ECLI:EU:C:2023:537]
- C-446/21. sz. ügy Ranthos főtanácsnok indítványa: Maximilian Schrems kontra Meta Platforms Ireland Limited, korábban Facebook Ireland Limited [ECLI:EU:C:2024:366]
- C-487/21. sz. ügy F. F. kontra Österreichische Datenschutzbehörde, a CRIF GmbH részvételével [ECLI:EU:C:2023:369]
- C-634/21. sz. ügy OQ és a Land Hassen között, a SCHUFA Holding AG részvételével folyamatban lévő eljárásban [ECLI:EU:C:2023:957]
- C-604/22. sz. ügyben hozott ítélet: IAB Europe és a Gegevensbeschermingsautoriteit között [ECLI:EU:C:2024:214]
- C-693/22. sz. ügy Pikamäe főtanácsnok indítványa: I. sp. z o. o. kontra M. W. [ECLI:EU:C:2024:162]

Magyar alkotmánybírósági határozatok:

- 32/2013. (XI. 22.) AB határozat
- 3110/2013. (VI. 4.) AB határozat
- 28/2014. (IX. 29.) AB határozat
- 3441/2020. (XII. 9.) AB végzés
- 15/2022. (VII. 14.) AB határozat

Magyar bírósági döntések:

- BH 2021.5.148.
- BH 2022.7.189.
- BH 2023.3.65.
- A Szegedi Ítélőtábla Pf.20282/2022/5. számú határozata
- A Fővárosi Ítélőtábla Pf.20258/2023/4. számú határozata

Amerikai bírósági döntések:

- John v. Clearview AI, Inc., 1:20-cv-03481 (District Court, S.D. New York, 2020)

- Acaley v. Vimeo, Inc., 464 F. Supp. 3d 959, 969 (N.D. Ill. 2020)
- L. v. Alphabet Inc. Alphabet Inc., 3:23-cv-03440 (N.D. Cal. 2023)
- P.M. v. OpenAI LP, 3:23-cv-03199 (N.D. Cal. 2023)
- Fed. Trade Comm'n v. Rite Aid Corp., 2:23-cv-05023 (E.D. Pa. Dec. 19, 2023)
- The New York Times Company v. Microsoft Corporation, 1:23-cv-11195 (District Court, S.D. New York, 2023)

Adatvédelmi hatóságok döntései, iránymutatásai, ajánlásai:

Az Adatvédelmi Munkacsoport, az Európai Adatvédelmi Hatóság és az Európai Adatvédelmi Biztos iránymutatásai, állásfoglalásai:

- EDPB, Endorsed WP29 Guidelines, https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en
- Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, Adopted on 20 June, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. 10.
- Adatvédelmi Munkacsoport 03/2014. sz. vélemény személyes adatok megsértése bejelentéséről, 693/14/EN, WP 213, elfogadva: 2014. március 25, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_hu.pdf
- Adatvédelmi Munkacsoport 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról, 844/14/HU, WP 217, elfogadás időpontja: 2014.04.09, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf
- Az Adatvédelmi Munkacsoport automatizált döntéshozatallal és profilalkotással kapcsolatos wp251.rev.01 sz 2017. október 3-án meghozott, 2018. február 6-án felülvizsgált iránymutatása
- Adatvédelmi Munkacsoport iránymutatása az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentéséről, 18/HU, WP250rev.01, elfogadás időpontja: 2017. október 3., a legutóbbi felülvizsgálat és elfogadás időpontja: 2018. február 6. https://ec.europa.eu/newsroom/article29/redirection/document/83862
- Az Adatvédelmi Munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti átláthatóságról, 17/HU, WP260 rev.01, elfogadás időpontja: 2017. november 29, a legutóbbi felülvizsgálat és elfogadás időpontja: 2018. április 11.

- Az Európai Adatvédelmi Testület 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat, elfogadás időpontja: 2020. október 20.
- Az Európai Adatvédelmi Testület 5/2020 Iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 1.1 verzió, elfogadás időpontja: 2020.05.04.
- Az Európai Adatvédelmi Testület 07/2020. sz. iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról, 2.0 változat, elfogadva: 2021.07.07.
- 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 rendeletre irányuló javaslatról. 2021.06.18.
- Az Európai Adatvédelmi Testület 3/2022. számú iránymutatása a sötét megoldásokról a közösségi média platformok felületein: hogyan ismerhetők fel és kerülhetők el, 1. verzió, 2022.03.14.
- EDPB, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Adopted on 17 April 2024
- EDPS, Data Protection Officer (DPO), https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Angol adatvédelmi hatósági döntések, iránymutatások, közlemények:

- ICO, Freedom of Information Act 2000 (FOIA) Decision Notice, 2022.02.08, https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4019607/ic-80804-j7c6.pdf
- ICO, Can we identify an individual indirectly from the information we have (together with other available information)?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/can-we-identify-an-individual-indirectly/
- ICO, Chapter 5: Privacy-enhancing technologies (PETs). Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. September 2022, https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

- ICO, Generative AI first call for evidence: The lawful basis for web scraping to train generative AI models, https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/generative-ai-first-call-for-evidence
- ICO, How do we ensure lawfulness in AI?, What about inferences and affinity groups?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/
- ICO, How to use AI and personal data appropriately and lawfully, https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf
- ICO, Penalty Notice, COM0804337, Marriott International Inc., 30 October 2020
- ICO, What are 'controllers' and 'processors'?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#:~:text=Employees%20of%20the%20controller%20are,data%20on%20the%20controller's%20behalf

Ír adatvédelmi hatósági döntések és iránymutatások:

- DPC, Should back-up data be considered as part of an access request?, https://www.dataprotection.ie/en/faqs/access-and-rectification/should-back-data-be-considered-part-access-request
- DPC, Guidance on the Use of CCTV – For Data Controllers, version last updated: May 2019, https://www.dataprotection.ie/sites/default/files/uploads/2019-05/CCTV%20guidance%20data%20controllers_0.pdf
- DPC, Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR, October 2019, http://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide
- DPC: Guidance Note. Data Protection in the Workplace: Employer Guidance. April 2023. 4.

Német adatvédelmi hatósági döntések, iránymutatások, közlemények:

- Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Einstieg ins Datenschutzrecht für behördliche Datenschutzbeauftragte, 2018.10.19,

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/10/Vortrag-f%C3%BCr-DSB_Verwaltungsschule.pdf

- Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2021, https://www.datenschutz-berlin.de/infothek/publikationen/jahresberichte/
- Sächsische Datenschutz- und Transparenzbeauftragte, Tätigkeitsbericht, Datenschutz, 2022, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2022.pdf
- Berliner Beauftragte für Datenschutz und Informationsfreiheit, Computer sagt Nein, 2023.05.31, https://www.datenschutz-berlin.de/pressemitteilung/computer-sagt-nein/
- Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Legal bases in data protection for the use of artificial intelligence, Discussion paper. Version 1.0, 2023.11.07, https://www.baden-wuerttemberg.datenschutz.de/legal-bases-in-data-protection-for-ai/
- Bayerisches Landesamt für Datenschutzaufsicht, Datenschutzkonforme Künstliche Intelligenz, Checkliste mit Prüfkriterien nach DS-GVO, 2024.01.24, https://www.lda.bayern.de/media/ki_checkliste.pdf

Magyar adatvédelmi hatósági döntések:

- NAIH/2015/2201/17/H.
- NAIH/2019/55/5. 17.
- NAIH/2019/1859.
- NAIH/2020/1154/9.
- NAIH/2020/2204/8.
- NAIH/2020/2729/15. 10.
- NAIH-3151-2/2021.
- NAIH-3975-1/2021.
- NAIH-963-10/2022.
- NAIH-3195-11/2022.
- NAIH-2732-2/2023.

Olasz adatvédelmi hatósági közlemények:

- Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l. - 22 luglio 2021 [9685994], https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994
- Garante, Provvedimento dell'11 gennaio 2024 [9977020], https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020
- Garante, Avviso di indagine conoscitiva in materia di webscraping, 2024.01.18, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9972153
- Garante, Intelligenza artificiale, il Garante privacy avvia istruttoria su “Sora” di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo, 2024.03.08, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9991867

Egyéb adatvédelmi hatósági döntések, iránymutatások, közlemények:

- AEPD, Artificial Intelligence: Transparency, https://www.aepd.es/en/prensa-y-comunicacion/blog/artificial-intelligence-transparency
- AEPD, GDPR compliance of processings that embed Artificial Intelligence. An Introduction, February 2020, https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf
- AEPD, Synthetic data and data protection, 2023.11.02, https://www.aepd.es/en/prensa-y-comunicacion/blog/synthetic-data-and-data-protection
- Autoriteit Persoonsgegevens, Richtlijnen scraping door private organisaties en particulieren, https://autoriteitpersoonsgegevens.nl/uploads/2024-05/Handreiking%20scraping%20door%20particulieren%20en%20private%20organisaties.pdf
- Autorité de protection des données, Décision sur le fond 21/2022 du 2 février 2022, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022.pdf
- CNIL, AI how-to sheets. Ensuring the lawfulness of the data processing, https://cnil.fr/en/ensuring-lawfulness-data-processing
- Datatilsynet, Artificial intelligence and privacy, Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

- Datatilsynet, Time for generative AI in the sandbox, https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/time-for-generative-ai-in-the-sandbox/
- Swedish Authority for Privacy Protection, Administrative fee against Spotify, 13 June 2023, https://www.imy.se/en/news/administrative-fee-against-spotify/