Pázmány Péter Katolikus Egyetem

Jog- és Államtudományi Doktori Iskola

dr. NECZ Dániel

A SZEMÉLYES ADATOK VÉDELMÉNEK LEGÚJABB KIHÍVÁSAI, KÜLÖNÖS TEKINTETTEL A DIGITALIZÁCIÓRA ÉS A MESTERSÉGES INTELLIGENCIA SZABÁLYOZÁSÁRA

doktori értekezés

Témavezetők:

Dr. KOLTAY András (egyetemi tanár)

Dr. PÉTERFALVI Attila (egyetemi tanár)

Budapest, 2023

Tartalomjegyzék

1. Bevezetés

Napjainkban az információ kiemelt értékkel bír, és az információs társadalom mozgatórugójává vált. Sok esetben az információ már nem csak az egyes szolgáltatásokhoz, tevékenységekhez kapcsolódó melléktermék, hanem a társadalom vagy a gazdaság, 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 intelligenciára (MI) támaszkodó alkalmazás képes pontosabb találati értékeket adni, és felhasználói igényeinket jobban kielégíteni. Mindennek oka, hogy az MI és egyéb forradalminak tekinthető technológiai megoldások ezen technológiák jellemzően nagyfokú adatéhségének folyamatos kielégítése mellett fejleszthetők csak tovább és alkalmazhatók sikeresen.

Az új technológiák és a velük kapcsolatos társadalmi és gazdasági jelenségek azonban a személyiségi jogok, és ezen belül a személyes adatok védelmét is új kihívás elé állítják, lévén, hogy az új technológiák általi, jellemzően tömegesen végzett adatfeldolgozás számos olyan adatot érint, amely kapcsán, illetve amelyben személyek tömege bír változatos jogokkal és érdekekkel.[2] Emellett továbbá a személyiségi jogok évszázadokkal korábban lefektetett keretrendszerének és az ezzel kapcsolatban kialakult jogalkotói és jogalkalmazói értelmezésének immár egy merőben új társadalmi, technológiai és gazdasági környezetben szükséges helytállnia, amely folyamatos újragondolást és 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

[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, Edmund Elgar Publishing, Cheltenham, Northampton, 2020. 391-410, 391.
[2] Chris Reed: Data Trusts for Lawful AI Data Sharing. In: Gary Chan Kok Yew, Man Yip (ed.): AI, Data and Private Law, Translating Theory into Practice, Hart Publishing, 2021, 47-68. 48.

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?

A jelen dolgozatban a fenti kérdésekre keresem a választ, különös hangsúllyal a fentiek kapcsán arra is, hogy a személyes adatok védelme hogyan garantálható a technológiai fejlődés támogatása, és így a versenyképesség megőrzése, valamint az adott technológia pozitív hatásainak maximális kihasználása mellett, illetve, hogy a személyes adatok védelme hogyan alkalmazható rugalmasan az egyes technológiák – különösen a társadalmi és gazdasági szerepe miatt kiemelkedőnek tekintendő MI – sajátosságaira is tekintettel. Továbbá a dolgozatban jelentős figyelmet szentelek az európai és amerikai szabályozás egyes vívmányainak, valamint sajátosságainak bemutatására. Ennek tükrében a részletes jogösszehasonlítástól eltekintek, azonban figyelembe veszem az egyes területek szabályozásának jellemzőit, és kitérek az azokkal kapcsolatos lehetséges előnyökre és hátrányokra is. Ezen kérdések megválaszolásához azonban szükséges a főbb technológiai fogalmak tisztázása, társadalmi hatásainak és etikai szempontjainak, valamint a jelenlegi, kialakuló szabályozás és egyben a szabályozási nehézségek ismertetése, amelyben a következő fejezetben kerítünk sort.

2. A digitalizáció és a mesterséges intelligencia meghatározása, társadalmi szerepe

A digitalizáció és a mesterséges intelligencia jelentős változásokat hoztak el társadalmunkban. Ezen változások jelentős részben pozitívnak mondhatók. Az online térben a korábbiakhoz nem fogható mértékben szabadon fejezhetjük ki véleményünket, érzéseinket, és egyben személyiségünket, valamint léphetünk kapcsolatba más emberekkel. A digitalizáció emellett a gazdaság számára is számos pozitív hatással jár, hiszen segítségével a szolgáltatók könnyebben érhetik el a fogyasztókat, és mutathatják be termékeiket és szolgáltatásaikat. Emellett a digitális technológia forradalmasította az internethasználók számára elérhető információk mennyiségét és minőségét is,[3] az MI-nek hála pedig számos feladat könnyebben elvégezhetővé vált és számos folyamat felgyorsult, így az emberi munkaerő a komplexebb, kreatívabb feladatok felé fordítható, miközben a technológiában rejlő gazdasági lehetőségek korábban soha nem látott változásokkal kecsegtetnek.

[3] Marilena Garis, Meeting the challenges of digitalisation, Managing intellectual property, 0960-5002. issue 199. (2010). 88-90. 88.

Mindemellett azonban a digitalizáció, valamint az MI és az azokhoz kapcsolódó egyes jelenségek vagy alkalmazások jelentős veszélyekkel is járhatnak a társadalom számára, valamint alkalmasak lehetnek arra, hogy a sérülékenyebb társadalmi csoportok tagjait (például: gyermekek, kevésbé informáltak, pszichológiai betegségben szenvedők) befolyásnak tegye ki vagy számukra olyan tartalmakat jelenítsen meg, amelyek adott esetben káros következményekhez vezetnek. Erre tekintettel vitathatatlan tény, hogy mind a digitalizáció vívmányai, mind az MI szabályozása számára egy olyan szabályozási keretrendszer kialakítása szükséges, amelyben az új technológiák dinamikus módon fejleszthetők és hasznosíthatók, azonban a káros hatások megelőzhetők vagy megfelelő időben és módon kiszűrhetők, így garantálva, hogy a digitalizáció és az MI fémjelezte jövő az emberiség egy sikeres újabb korszakát hozhassa el.

a. A digitalizáció jelentése és hatása a társadalomra

A digitalizáció, amely a különböző digitális szolgáltatások és megoldások gazdaságba való bekapcsolását, a gazdaság és az üzleti vállalkozások technológiai forradalom adta működtetését, felélénkítését[4] valósítja meg, jelentős hatással van a társadalom működésére, valamint a társadalmi-gazdasági folyamatok alakulására. Segítségével a tudás szélesebb körben válik elérhetővé, a megszámlálhatatlan mennyiségű információ tulajdonképpeni privatizálásával pedig javíthatók az egyéni képességek, továbbá új szolgáltatások nyújthatók, termékek fejleszthetők és együttműködések alakíthatók ki. A digitális gazdaság[5] fejlődése a fentiekkel összhangban egyben az adatgazdaság[6] kialakulásához is vezetett, amelynek keretében a vállalkozások már kiemelten a jelentős adattömegek összegyűjtése, megosztása, valamint az adatok elemzése, kiértékelése, felhasználása révén valósítják meg gazdasági céljaikat.

[4] Digitalization, Gartner Glossary, Gartner, https://www.gartner.com/en/information-technology/glossary/digitalization [2023.04.23.]
[5] Digitális gazdaságnak nevezzük a digitális interakciókra, adatmegosztásra épülő gazdaságot. Lásd: Deloitte, What is digital economy? https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html [2023.09.05.]
[6] Egy olyan világszintű globális ökoszisztéma, ahol adatokat termelő és felhasználó személyek és szervezetek számos forrásból gyűjtenek, illetve dolgoznak fel és osztanak meg adatokat. Lásd: Capitalizing on the data economy, MIT Technology Review Insights, 2021.11.16, https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/ [2023.09.05.]

Napjaink digitális társadalmában, illetve gazdaságában az információk megtalálásához kiemelt segítségül szolgálnak a keresőszolgáltatások, mint például a Google, a Bing vagy a Yahoo nevű keresőoldalak, illetve a különböző online könyvtárak és adatbázisok (például: tudományos kutatáshoz használt adatbázisok, egyetemek, könyvtárak adatbázisai), míg a videómegosztó platformok, mint például a YouTube segítségével számos videótartalom osztható meg változatos célokból. A digitalizáció továbbá segítséget nyújt a kapcsolatépítésben és az önkifejezésben is. Erre kiemelt például szolgálnak a közösségi médiaoldalak, amelyek az egyének baráti, személyes kapcsolatépítésén túl akár kereskedelmi célokra, fogyasztók közti tranzakciókra (például: Facebook Marketplace) vagy szakmai kapcsolatok építésére, szakmai reputáció növelésére is használhatók (például: LinkedIn).

Mindemellett a digitalizáció a vásárlást, az utazást és a különböző szolgáltatók közti választást is átalakította, és sok szempontból megkönnyítette a fogyasztók többsége számára, ideértve különösen az online piactereket (például: Amazon) vagy a szállásfoglaláshoz használt megoldásokat (például: Airbnb vagy booking.com), és átalakította a társkeresési, párválasztási szokásokat is (például: Tinder vagy az LMBTQ közösség tagjai körében népszerű Grinder elnevezésű társkereső applikációk).

A fentieken túl napjaink digitális gazdaságában a platformszolgáltatók jellemzően egy platformot (különösen: weboldal, applikáció) nyújtanak a fogyasztók vagy más szolgáltatásokat, termékeket keresők és az ezen szolgáltatásokat és termékeket kínáló személyek, szervezetek részére. Tekintettel azonban arra, hogy az egyes platformok az elmúlt időszakban meghatározóvá váltak, így az adott iparági szereplők vagy szolgáltatás, illetve terméktípusok nyújtói és az ezen termékeket vagy szolgáltatásokat keresők számára szinte kizárólagossá vagy nehezen helyettesíthetővé váltak, így a platformszolgáltatók a domináns gazdasági pozícióból eredő gazdasági előnyökön túl egyfajta irányító szerepbe is léptek, sok esetben szabadon döntve arról, hogy az adott platformon és ahhoz kapcsolódóan a keresőoldalakon keresztül milyen termékek vagy szolgáltatások érhetők el. Ezentúl jelentős beleszólással bírnak azzal kapcsolatban, hogy az adott iparágban mely szolgáltatók termékei vagy szolgáltatásai jutnak el több emberhez. Mindez értelemszerűen jelentős visszaélésekhez is vezet (ideértve például az alább említett „shadow banning” vagy egyéb visszaélésszerű gyakorlatokat), miközben a fenti irányítói vagy kapuőri szerepet betöltőkkel szemben kevés jogszabályi elvárás érvényesül. Ezen helyezetek igazságosabb rendezésére és a felelősség

hatékonyabb megragadására az Európai Unión belül is több jogszabály, illetve jogszabály-tervezet született, amelyekről alább írunk részletesebben.

A fentieken túl szintén jelentős problémát jelent a monopolisztikus helyzetben lévő szolgáltatók egyes tartalmainak, szolgáltatásainak elérhetőségi korlátozása (angolul: „*walled garden*"), amely megoldással ezen szolgáltatók korlátozzák a fenti tartalmak vagy szolgáltatások egyéb felületeken való elérhetőségét.[7] Mindezzel ugyan a szolgáltatók sok esetben jogosan védhetik a jelentős gazdasági értéket képviselő egyes tartalmaikat a jogosulatlan felhasználással szemben, azonban ezáltal egyben bizonyos tartalmak vagy szolgáltatások körét lényegében kizárólag a saját felületeikre korlátozzák, ezzel egyben csökkentve a versenyt, valamint sokszor jelentős díjfizetési kötelezettséget támasztva a felhasználókkal szemben.

A digitalizált társadalomban ugyanakkor szintén meghatározó jelenségnek számítanak az online reklámok, amelyek segítségével a vállalkozások számos fogyasztót képesek megszólítani, ez ugyanakkor bizonyos esetekben a fogyasztók jogait is sértheti (például: félrevezető reklámok), illetve számukra sok esetben zavaróan hathat. Emellett napjainkra a reklámipar szerves részévé váltak a profilalkotás eredményeként létrejött személyre szabott reklámok, amelyek segítségével még közvetlenebbül szólíthatók meg a fogyasztók (ideértve például: bizonyos korosztályra, társadalmi csoportra szabott reklámok, inaktív vásárlók megcélzása). Mindez azonban bizonyos esetekben a fogyasztók manipulációjához, kihasználásához, valamint a személyes adatok beláthatatlan módon és célokra történő kezeléséhez vezethet, amely kockázatok egyúttal a személyes adatok, valamint a fogyasztók jogainak hatékonyabb védelmét követelik meg.

A fenti kockázatok mellett azonban az online tér egyéb kockázatokat, veszélyeket is rejt, amelyek sok esetben a kiber-, valamint az „offline" bűnözéssel fonódnak össze. E körbe tartozik az ún. sötét web (angolul: „dark web"), amely egy az internet egy meghatározott, ún. Tor elnevezésű alkalmazáson elérhető, mélyebb, nem publikus rétegét jelenti, amelyre a magas fokú anonimitás jellemző. A sötét weben keresztül pedig a legális tevékenységen és kommunikáción túl illegális tevékenység és szolgáltatásnyújtás is történik (például: kábítószerkereskedelem, illegális tartalmak, lopott bankkártyaadatok megosztása, értékesítése). Mindezt az Edinburgh-i Egyetem egy végzős hallgatója, Ian Clarke „Freenet" elnevezésű projektje alapozta meg 2000-

[7] PCMag.com, Encyclopedia, Walled Garden, https://www.pcmag.com/encyclopedia/term/walled-garden [2023.08.13.]

ben, amelyet a Tor projekt, majd az annak alapján létrejött böngészőoldal követett.[8] Részben hasonló szellemben hozta létre – legalábbis saját szavai alapján – a Silk Road (vagyis magyarul: Selyemút) elnevezésű hálózatot a Ross Ulbricht nevű volt amerikai fizikus hallgató, amely rövid időn belül egy főként internetes drogterjesztésre szolgáló hálózattá nőtte ki magát, több mint százmillió dolláros forgalmat bonyolítva, egyben személyes tragédiákhoz is vezetve egyes felhasználók túladagolása révén; mindez alapján végülis az alapítót az illetékes amerikai bíróság tényleges életfogytiglani szabadságvesztésre ítélte.[9] Emellett az elmúlt években egyfajta szürke zóna is kialakult a sötét web és a legális internet között, amely hasonlóan súlyos veszélyeket rejt, és számos esetben kínál a sötét webhez hasonló káros tartalmakat.[10]

A sötétweben és az azt övező „szürke zónán" kívül azonban további veszélyeket is rejthet magában az online tér, ideértve például az álhíreket (angolul: „*fake news*"), valamint az ezekkel kapcsolatos hamis, illetve megmásított tartalmakat. Az álhírek esetén különös veszélyt jelent, hogy ezek jellemzően a társadalom egy kisebb vagy nagyobb csoportjának félelmeire, nézeteire vagy ellenérzéseire építve hoznak létre összeesküvés-elméleteket vagy erre építő mozgalmakat, amelyek alapvetéseit, kijelentéseit éppen érzelmi kötődésük okán a tényszerűség alapján, logikai érvekkel nehéz megcáfolni. Erre jó példának tekinthető a korábbi években elterjedt QAnon mozgalom, amelynek alapvetése szerint a korábbi amerikai elnök, Donald Trump egy befolyásos, üzletemberekből, demokrata politikusokból és döntéshozókból álló sátáni és pedofil összeesküvés ellen harcol, így az őt ért támadások, vele kapcsolatos eljárások, kritikák is ezen összeesküvésre vezethetők vissza. A mozgalom teóriái és a vele kapcsolatos tartalmak, szlogenek és ábrák az internet és a közösségi média hatására felhasználók millióihoz jutottak el, a mozgalom követői pedig részt vettek a 2021. januárjában a Kapitólium elleni „ostromban" is.[11]

Érthető módon az álhírek ellen a leghatásosabb védelemnek a tájékozottság és az oktatás tekinthető, azonban szintén fontos intézkedésnek számít a közösségi média oldalakon és egyéb felületeken az álhírek jelentésének lehetősége, valamint ezek üzemeltetőinek, szolgáltatóinak

[8] Everything You Should Know About the Dark Web, Tulane University School of Professional Advancement, https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web [2023.04.23.]
[9] Sam Thielman, Silk Road operator Ross Ulbricht sentenced to life in prison, https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced [2023.04.25.]
[10] Gyekiczky Tamás, Jogrendszerek a Digitális Társadalomban, Wolters Kluwer Hungary Kft., Budapest, 2020. 107.
[11] Mike Wendling, QAnon: What is it and where did it come from? BBC News, 2021.01.06, https://www.bbc.com/news/53498434 [2023.04.26.]

intézkedései a káros tartalmak eltávolítása kapcsán. Ebből a szempontból azonban a cenzúra problémája is felmerül, hiszen a megosztóbbnak tekinthető hangokat megütő közszereplők vagy egyéb felhasználók eltávolítása, korlátozása egyben szűkíti is a társadalmi párbeszéd és a demokratikus vita lehetőségét. A fenti kritikákra való reagálásként döntött úgy a Facebook, hogy létrehoz egy különböző hátterű szakértőkből álló Ellenőrző Bizottságot (angolul: „*Oversight Board*") a Facebook, valamint az Instagram véleménynyilvánítás szabadságát korlátozó döntéseinek felülvizsgálata kapcsán. A Bizottság 2020-ban kezdte meg a működését, és jellemzően számos eset közül választja ki a legnehezebbnek vélteket, amelyek kapcsán akár a Facebook (vagy 2021. végétől új nevén: Meta) korábbi döntését is felülbírálhatja. Ezen kívül ajánlásokat tehet a Meta számára, amelyekre az a nyilvánosság előtt is reagál.[12] A fenti törekvések ellenére is azonban számos olyan eset fordult elő, ahol az adott közösségi médiatartalom szolgáltató egy-egy megosztónak vélt véleményvezér letiltása, illetve elérhetőségének korlátozása mellett döntött vagy ennek gyanúja merült fel. Trump volt amerikai elnököt több közösségi médiaoldal is letiltotta a 2021. januári kapitóliumi zavargások, illetve Trump elnök megosztónak vélt megjegyzései okán. A Meta például az Ellenőrző Bizottság döntését is figyelembe véve határozott úgy, hogy két év elteltével 2023-tól „visszaengedi" a korábbi elnököt a felületeire.[13]

Megemlítendő továbbá, hogy egyes esetekben az egyértelmű letiltáson túl bizonyos felhasználók, illetve közszereplők az adott közösségi médiaoldalon való elérhetőségük korlátozására (angol kifejezéssel: „*shadow banning*") is panaszkodtak, ideértve például Varga Judit magyar igazságügyi minisztert is.[14] A magyar Igazságügyi Minisztérium például egy Digitális Szabadság Bizottság nevű szervezetet is létrehozott 2020-ban, amely az érintett hatóságok, illetve szakértők bevonásával vizsgálja a multinacionális technológiai vállalatok, különösen a közösségi médiaszolgáltatók működését és annak egyes jogi és társadalmi aspektusait.[15] Ennek kapcsán további kérdéseket vethet fel az egyes platformok, közösségi médiaoldalak hirdetési, tartalommegjelenítési gyakorlata, amely az egyes tartalmak korlátozása mellett más tartalmak személyre szabott elérhetőségét és megjelenítését is biztosítja a

[12] Oversight Board, https://www.oversightboard.com/appeals-process/ [2023.04.26.]
[13] Noor Nanji, Donald Trump to be allowed back on to Facebook and Instagram, BBC News, 2023.01.26, https://www.bbc.com/news/business-64408306 [2023.04.26.]
[14] Gergely Szakacs, Hungary mulls sanctions against social media giants, Reuters, Technology News, 2021.01.18, https://www.reuters.com/article/us-hungary-media-regulations-idUKKBN29N1BV [2023.04.26.]
[15] Digitális Szabadság Bizottság, https://digitalisszabadsag.kormany.hu/ [2023.04.26.]

felhasználók számára, adott esetben kevésbé átláthatóan, illetve a felhasználók befolyásolása mellett.[16]

A szólásszabadság korlátozása, valamint a személyre szabott hirdetések és egyéb tartalmak mellett további veszélyeket jelentenek az online térben az álhírek és deepfake tartalmak, az ezek elleni küzdelem azonban bizonyos esetekben ütközhet a véleménynyilvánítás szabadságával, ugyanis a népszerűtlenebb nézeteket megjelenítő tartalmakat, valamint azokat megjelenítő véleményvezéreket is eltávolításra szántnak ítélheti, illetve száműzheti, míg a deepfake tartalmak egy része kapcsán is jelentkezhetnek olyan elemek, ahol a szólásszabadság és a kritikus véleménynyilvánítás erőteljesebben képviselteti magát (például: parodisztikus vagy kritikusnak szánt művek). Éppen ezért az első látásra hamisnak tűnő tartalmak egy része kapcsán is fontos, hogy a szabályozás, valamint a szolgáltatók általi tartalomkorlátozás is kizárólag a káros, illetve félrevezető tartalmak megfékezését, elérhetetlenné tételét célozza, mivel a parodisztikus, kritikai jellegű, illetve hasonlóan demokratikus közbeszéd részét képező tartalmak korlátozása komoly alapjogi aggályokat vethet fel, ahogyan a kisebbségi vélemények csorbítása is a domináló vélemény birtokosa által, vagy annak érdekében.[17] Ugyanakkor a fenti körbe nem tartozó, illetve kifejezetten félrevezetés céljára készített tartalmak kapcsán ilyen demokratikus védelemről nem beszélhetünk. 2022. elején, az Ukrajna elleni orosz invázió nyitányakor például Putyin orosz elnökről megjelent egy deepfake videó a Twitteren, amelyen az orosz elnök békét hirdet, mindemelett Zelenszkij ukrán elnök kapcsán a Meta és a YouTube is eltávolított egy deepfake videót, amelyen az elnök fegyverletételről beszél.[18] 2023. elején emellett például egy Joe Biden amerikai elnökről készült videó terjedt el a közösségi médiában, amelyen az elnök a transzneműeket sértő megjegyzéseket tesz; a videót szakértők deepfake-ként azonosították.[19] A fentiekhez hasonló tartalmak napjainkban egyre elterjedtebbnek számítanak, különösen világvezetők esetén, a cél pedig egyértelműen dezinformációs jellegű (például: választási manipuláció vagy félelemkeltés).

[16] Koltay András, Az új média és a szólásszabadság. A nyilvánosság alkotmányos alapjainak újragondolása, Wolters Kluwer Hungary Kft., Budapest, 2019. 204.
[17] Cserván Csaba, A digitalizáció hatása az alapjogok hatására és érvényesítésére. In: Homicskó Árpád Olivér (szerk.), A digitalizáció hatása az egyes jogterületeken, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, 2020. 55-76. 56.
[18] Jane Wakefield, Deepfake presidents used in Russia-Ukraine war, BBC News, 2022.03.18, https://www.bbc.com/news/technology-60780142 [2023.04.29.]
[19] Fact Check-Video does not show Joe Biden making transphobic remarks, Reuters, Reuters Fact Check, 2023.02.10, https://www.reuters.com/article/factcheck-biden-transphobic-remarks-idUSL1N34Q1IW [2023.04.29.]

A dolgok internete (angolul: „*Internet of Things*”, röviden: „*IoT*”), vagyis a technikai, különösen az okoseszközök (például: okostelefon, járművek, háztartási eszközök, stb.) közötti kapcsolatot biztosító internetes hálózatok, illetve kommunikáció[20] szintén jelentős változásokat hozott, amelyek adatvédelmi szempontból is jelentőséggel bírnak, tekintettel arra, hogy ezen eszközök jellemzően nagy mennyiségű adatot osztanak meg (ideértve sok esetben személyes adatokat is) automatizált módon. A fentiteken túl az automatizált kommunikációra, valamint az adatok és ezen kommunikáció védelmének fontosságára tekintettel szintén jelentős szempontot képvisel az IoT eszközök esetén az adatbiztonság, amellyel kapcsolatos legfontosabb elvárásokat – az adatvédelmi jogszabályi rendelkezéseken túl – az adott eszközökre, valamint iparágra irányadó szabályozás, illetve az irányadó iparági gyakorlat írja elő, és foglalja össze, így az irányadó adatvédelmi szabályok és elvárások is csak ezekkel, valamint a vonatkozó technológiai feltételekkel összhangban érvényesülhetnek. Ezen eszközök még jelentősebb szerepet játszanak az okosvárosok fejlesztése esetén, ideértve olyan helyeket, illetve településeket, ahol a hagyományos hálózatokat és szolgáltatások digitális megoldásokkal erősítik, e körbe értve például a közlekedésszervezést, az ivóvízgazdálkodást, a közfűtést és közvilágítást vagy épp a hulladékgazdálkodást.[21] Ennek kapcsán kiemelt jelentőséggel bírnak az adott területen alkalmazott kamerarendszerek, ugyanis a kameraképek kapcsán kiemelt jelentőséggel bíró kép- és videófeldolgozás révén[22] a szolgáltatások minősége sok esetben javítható, az esetleges hibák pedig elháríthatók, az egyes tevékenységek hatékonyabban végezhetők.

A digitális gazdaság tekintetében ugyancsak forradalmat jelentett a blokklánc (angolul: „*blockchain*”) technológia, amely először a kriptovaluták területén jelent meg, majd számos egyéb megoldás és technológiai vívmány, szolgáltatás és vállalkozás számára is alapul szolgált. A blokklánc lényegében egy elosztott főkönyvi rendszer, ahol az egyes tranzakciók egymáshoz kapcsolódó blokkokban jelennek meg. A blokklánc sajátossága, hogy a közvetítő szerepet (például: bankok, brókerek) teszi szükségtelenné, dinamikáját pedig jellemzően a blokklánchoz kapcsolódó okosszerződések (angolul: „*smart contracts*”) – azaz a blokkláncon tárolt, automatikusan végrehajtásra kerülő szabályok – adják.[23] A blokklánc technológia alapjait az

[20] European Data Protection Supervisor, Internet of Things, https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en [2023.08.12.]
[21] European Commission, Smart cities, https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en [2023.09.12.]
[22] Szűcs Gábor, Sallai Gyula, Az okos város kameraképeinek elemzése, Dialóg Campus Kiadó, Budapest, 2019. 69.
[23] IBM, What is blockchain technology? https://www.ibm.com/topics/blockchain [2023.08.01.]

első, és napjainkig legismertebb kriptovalutát, a Bitcoin-t és működését leíró, 2008. végén publikált tanulmány[24] adja. A tanulmányt egy Satoshi Nakamoto álnevet használó szerző vagy szerzők publikálták, akinek vagy akiknek a személyét napjainkig nem sikerült felfedni. A Bitcoin árfolyama az elmúlt években a sokszorosára nőtt,[25] egyúttal számos egyéb kriptovaluta és azok kereskedésének helyt adó tőzsde vagy alkalmazás is megjelent, és elterjedté vált. Mindemellett azonban maga a blokklánc technológia is túlnőtt a kriptovaluták világán. Napjainkban használják például okos energiahálózatok, pénzügyi szolgáltatások, valamint számos egyéb tevékenység és megoldás kapcsán is. Emellett szintén egyre jelentősebb piacnak tekinthetők az ún. nem helyettesíthető token-ek (angolul: „*non-fungible token*", röviden: „*NFT*"), amelyek lényegében blockchain-alapú, tulajdont megtestesítő digitális jelölők vagy token-ek, amelyek tulajdont testesítenek meg valamely digitális eszköz vagy egyéb tartalom felett (ideértve például műalkotásokat).[26] A fentieken túl a különböző egyéb javak és értékek (akár nagy értékű, a fizikai világban létező műtárgyak vagy eszközök) tokenizációja is megfigyelhető, amellyel az ebben érdekelt vállalkozások vagy közösségek egy részvényhez hasonló részesedést megtestesítő jelölőt biztosítanak az abban érdekelt felhasználók részére.

Egyre inkább elterjedni látszanak továbbá a szintén blokklánc alapú decentralizált autonóm szervezetek (angolul: „*decentralized autonomous organizations*", röviden: „*DAO*"), amelyek a „klasszikus értelemben vett" jogi személyeknél lazább struktúrát követnek, és egy-egy meghatározott célból működő közösség akaratát testesítik meg, amelyben a közösség tagjai az egyes jogaikat „részvényhez" hasonló módon funkcionáló ún. token-ek révén gyakorolhatják.[27] Emellett napjainkban az internetet is egyre inkább illetik a „web3" kifejezéssel. Az eredetileg Gavin Wood blockchain vállalkozótól származó kifejezés az internetet, illetve az internet jövőjét egy sokkal inkább decentralizált működésként fogja fel, ahol az internet biztosítását már

[24] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf [2023.09.19.]
[25] Még 2010. nyarán egy Bitcoin egy dollárnál is kevesebbet ért, 2021. áprilisára egy Bitcoin ára meghaladta a 60.000 dollárt, majd 2022. végére az árfolyam 20.000 dollár alatt mérséklődött (John Edwards, Bitcoin's Price History, Investopedia, 2023.05.24, https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp [2023.09.06.])
[26] Gartner, Gartner Glossary, Non-Fungible Token (NFT), https://www.gartner.com/en/information-technology/glossary/non-fungible-token-nft [2023.08.13.]
[27] Kevin Roose, The Latecomer's Guide to Crypto, What are DAOs? The New York Times, Technology, https://www.nytimes.com/interactive/2022/03/18/technology/what-are-daos.html [2023.08.01.]

nem csak a nagy technológiai vállalatok végzik, így az internet működésébe és működtetésébe szélesebb közönségek is beleszólással bírnak.[28]

A fentieken túl kiemelendő, és napjainkban egyre nagyobb szerepet kap a „metaverzum" is, amely lényegében olyan digitális világként határozható meg, amelyhez a felhasználók mozgást, fizikai állapotot és sokszor érzelmeket is érzékelő eszközök útján csatlakoznak. A metaverzumban létező egyes „világok" sok esetben a „való" világ leképeződéseiként jelennek meg, így például városok épülnek bennük, ahol helyet kapnak bárok, kocsmák és egyéb virtuális terek, események, ahol a felhasználók találkozhatnak és különböző interakciókat végezhetnek. Ezenfelül akár ingatlant vagy más virtuális tárgyakat is vásárolhatnak az egyes világokban, valamint különböző szolgáltatásokat vehetnek igénybe (például: koncerten vagy különböző játékokban vehetnek részt). Ezekért a digitális tárgyakért, jogosultságokért, szolgáltatásokért a felhasználók jellemzően valamilyen kriptovalutával (azaz decentralizált digitális fizetőeszközzel, mint például a Bitcoin) fizetnek.

Értelemszerűen a metaverzum az egyéni felhasználók mellett a vállalkozások számára is rengeteg lehetőséget kínál, hiszen akár ismert világmárkákról, akár kisvállalkozásokról, tartalomgyártókról vagy közszereplőkről beszélünk, ezek a metaverzumon keresztül mind egy új szinten kapcsolódhatnak a fogyasztókkal, követőkkel, illetve általánosságban a társadalom tagjaival, közelebbről megismerhetik igényeiket, és elégíthetik azt ki személyre szabott szolgáltatások útján. Mindemellett azonban a metaverzum kapcsán számos kockázat és fenyegetés is felmerülhet az egyéni felhasználók számára, amelyek álláspontom szerint az általánosan alkalmazandó adatvédelmi, fogyasztóvédelmi rendelkezéseken túl speciális, a metaverzumra vonatkozó szabályozás útján is kezelendők. A kockázatok jelentős részben a végtelennek tekinthető adathalmazok építéséből, a felhasználók szokásait, érzelmeit soha nem látott pontossággal, szenzorokon át feltérképező megoldásokból és profilalkotásból származnak, amelyek kiemelt mértékű behatással bírhatnak a felhasználók magánéletébe, gondolataiba, valamint döntéseiket, viselkedésüket, érzelmeiket is nagy mértékben befolyásolhatják. Tekintettel ezen kockázatok, valamint a metaverzum adatvédelmi szempontjainak jelentőségére, ezeket a dolgozat egy külön alfejezetében ismertetjük.

[28] Arjun Kharpal, What is 'Web3'? Here's the vision for the future of the internet from the man who coined the phrase, CNBC, 2022.04.19, https://www.cnbc.com/2022/04/20/what-is-web3-gavin-wood-who-invented-the-word-gives-his-vision.html [2023.08.09.]

A fentiekre tekintettel jól látható, hogy napjainkra a digitalizáció vívmányainak köszönhetően mind társadalmunk, mind a világgazdaság merőben átalakult. Korunkban az információ egyúttal számos megoldás és szolgáltatás „alapanyagává" vált, amelynek hála a szolgáltatások soha nem látott mértékben szabhatók személyre, és elégíthetik ki elvárásainkat, valamint könnyíthetik meg az életünket.

A digitalizáció azonban számos előnyén túl kiemelt veszélyekkel is járhat a társadalom tagjai számára, hiszen az új technológiai megoldások révén soha nem látott pontossággal térképezhető fel az emberi személyiség, valamint szokásaink, meglátásunk és érzéseink, amely információk birtokában az egyénre jelentős befolyás gyakorolható, ideértve például a véleményformálás, vásárlási és fogyasztási szokások területét, a reklámipar hatásait vagy épp a választói akarat kifejezését. Emellett az online tér a kiberbűnözés, valamint számos online visszaélés (például: zaklatás, másokat sértő tartalmak megjelenítése) kapcsán is új kihívás elé állítja a szabályozókat. Ennek kapcsán mindenképp csak egy összetett, az online világ sajátosságait figyelembe vevő szabályozás lehet alkalmas a negatív hatások megfelelő megfékezésére, anélkül azonban, hogy a technológiai fejlődést visszafogná, vagy annak pozitív hatásait túlzott mértékben csorbítaná.

b. 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 sziget védelmére.[29] 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 vált szenzációvá, amelyben azonban valószínűleg egy emberi kezelő lapult. Később egyre inkább az irodalom és a filmipar foglalkozott a mesterséges intelligenciával, és különösen annak testet öltött formájával, a robotokkal.[30] Erre jó példának tekinthető Mary Shelley 19. század elején írt, Frankenstein című

[29] 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/ [2023.03.08.]
[30] A mesterséges intelligencia irodalom- és filmtörténeti hivatkozásaihoz lásd: Necz Dániel, A mesterséges intelligencia hatása a szerzői jogra, Iparjogvédelmi és Szerzői Jogi Szemle, 123/6 (2018). 51-76. 52-53.

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 meghonosította.

Az egyik leghíresebb, illetve legismertebb irodalmi hivatkozásnak ebben a témában azonban kétségkívül az amerikai tudományos-fantasztikus író, Isaac Asimov munkássága tekinthető, ideértve különösen a robotika három alaptörvényét, amelyet Asimov 1942-ben megjelent, Körbe-körbe című novellájában[31] 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.[32]

A fenti irodalomtörténeti előzmények után a tudomány is egyre nagyobb figyelmet fordított a mesterséges intelligenciára.[33] Ezzel párhuzamosan már a 19. század folyamán, valamint a századforduló idején is egyre nagyobb lendületet vett a számítástechnika fejlődése, valamint a számítógépek korszaka is egyre inkább közelségbe került. Charles Babbage, angol matematikus például a 19. század derekán álmodta meg a számítógép kezdeti koncepcióját, amely kapcsán az első algoritmust a szintén angol matematikusnak, Ada Lovelace-nek köszönhetjük, aki egyben az informatika első kimagasló női alkotójának is tekinthető.

A számítógép és az informatika létrehozásának első lépéseit követően a huszadik század derekán az MI-vel kapcsolatos fejlesztések is különös lendületet vettek. Ennek kapcsán kiemelt jelentőséggel bír Warren Mccollough és Walter Piths munkássága, akik az 1940-es években mesterséges genomokon alapuló elméletükkel sikeresen kimutatták, hogyan végezhetők

[31] 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, 1942, 29(1)

[32] Példaértékűnek tekinthető, különösen 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", 38th International Conference of the Data Protection and Privacy Commissioners, Marrakech, 2016.10.19. Elérhető: https://archive.epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf [2023.04.07.]

[33] A mesterséges intelligencia tudománytörténeti előzményei kapcsán lásd: Necz [30]. 53-55.

számítások, illetve állíthatók elő függvények egymással összekötött genomok hálózatával.[34] Emellett az MI tudományos megalapozása és mérése kapcsán kiemelt jelentőségűnek tekinthető a híres angol matematikusról, Alan Turingról elnevezett, ún. Turing-teszt. Ennek alapjait Turing az 1950-ben megjelent „Számítógép és értelem" című tanulmányában fektette le. Ez lényegében egy imitációs játékon alapul, amelyben egy „kérdező" és két másik „személy" vesz részt, egy ember és egy mesterséges intelligencia megoldás. A teszten akkor megy át a gépi válaszadó, vagyis a mesterséges intelligencia, ha elhiteti a kérdezővel, hogy ember.[35]

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.[36] 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 mesterséges intelligenciáról szóló konferencián is bemutatásra került a tudományos nagyközönség számára.[37] Ezt követően egyre több olyan alkalmazás jelent meg, amelyek természetes nyelvi feldolgozásra (angolul: „*natural language processing*") építenek, amelynek 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.[38] Nem sokkal később, 1966-ban jelent meg a Joseph Weinzbaum által készített, első chatbot alkalmazás, ELIZA is, amely egy pszichoterapeutával való beszélgetést imitált.[39] Hangsúlyozandó azonban, hogy az MI tanulási képességeit a kutatások ezen kezdeti időszakában kritikák is érték,

[34] Elek István: Az intelligencia spontán megjelenése. ELTE Eötvös Kiadó, Budapest, 2015. 32-33.
[35] Alan Mathison Turing: Computing Machinery and Intelligence. Mind, 59. évf. 236. sz., 1950. október. 433-460. 433-434.
[36] Siobhan Roberts, Christopher Strachey's Nineteen-Fifties Love Machine, 2017.02.14, https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine [2023.05.14.]
[37] Rockwell Anyoha: The History of Artificial Intelligence, Harvard SITN Blog, 2017.08.28, http://sitn.hms.harvard.
edu/flash/2017/history-artificial-intelligence/ [2023.04.07.]
[38] Daniel G. Bobrow, Natural Language Input for a Computer Problem Solving System, 1964.03.30, https://dspace.mit.edu/bitstream/handle/1721.1/5922/AIM-066.pdf?sequence=2&isAllowed=y [2023.05.14.], 4-6.
[39] ELIZA: a very basic Rogerian psychoterapist chatbot, https://web.njit.edu/~ronkowit/eliza.html [2023.04.07.]

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 beszélné a kínai nyelvet.[40] 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 könnyen juthatunk arra a következtetésre, hogy napjaink úttörőnek számító MI alapú megoldásai is inkább csak utánozzák az emberi értelmet, mintsem, hogy egy új, önálló intelligenciát képviseljenek.

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 lehetőségekkel járt, majd az ezt követő újabb fellendülést követően az 1990-as évekre egy második „MI tél” köszöntött ránk[41]. Természetesen azonban ezen időszaknak is számos vívmányt köszönhetünk. Az 1980-as és 1990-es évekre például a személyi számítógépek 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.[42] Ezt követően a mesterséges intelligencia 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.[43] A fejlődés egekbe szárnyaló íve pedig

[40] John R. Searle, Minds, brains and programs, The Behavioral and Brain Sciences 3/1980. doi:10.1017/S0140525X00005756. 417-457. 417-419.
[41] Blagoj Delipetrev, Chrisa Tsinaraki, Uroš Kostić, AI Watch, Historical Evolution of Artificial Intelligence. Analysis of the three main paradigm shifts in AI, 2020, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120469/jrc120469_historical_evolution_of_ai-v1.1.pdf [2023.06.25.]. 3.
[42] Delipetrev, Tsinaraki, Kostić [41]. 9.
[43] Delipetrev, Tsinaraki, Kostić [41]. 13.

napjainkra sem látszik megtörni. Az elmúlt időszakban például az OpenAI nevű nonprofit szervezet ChatGPT elnevezésű chatbot megoldása[44] 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 számos esetben továbbra sem nélkülözhető az MI által végzett munka emberi felülvizsgálata. Erre egy new york-i ügyvédi iroda által elkövetett kínos hiba világított rá 2023-ban. Az iroda ügyvédjei ugyanis 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.[45]

Ami a mesterséges intelligencia meghatározását illeti, itt sem beszélhetünk egységesen elfogadott definícióról, illetve minden tekintetben általánosan használt megközelítésről. A téma egyik úttörője, az amerikai kutató, John McCarthy a mesterséges intelligenciát például az intelligens gépek, és különösen intelligens komputer programok létrehozásának tudományaként határozta meg.[46] Ezzel szemben Elek István emberi módra, illetve logikusan gondolkodó gépek között tesz különbséget,[47] az MI céljaként pedig az intelligens entitások megértését és létrehozását jelöli meg.[48] 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.[49].

Az irodalmi meghatározásokon túl az MI és az ahhoz kapcsolódó egyes fogalmak jellemzően jogszabályi meghatározásokkal is bírnak. E tekintetben az irányadó jogszabályi meghatározásokat és megközelítéseket a dolgozat nemzetközi, európai uniós és amerikai

[44] ChatGPT, https://openai.com/blog/chatgpt [2023.04.07.]
[45] 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 [2023.06.25.]
[46] John McCarthy, What is Artificial Intelligence? 2007.11.12, http://www-formal.stanford.edu/jmc/whatisai/node1.html [2023.04.07.]
[47] Elek [34]. 22-23.
[48] Elek [34]. 21.
[49] Hubert L. Dreyfus, What Computers Still Can't Do. A Critical of Artificial Reason, The MIT Press, Cambridge, London, 1992. 119.

szabályozást tárgyaló alábbi részeiben ismertetjük. A fentieken túl az MI meghatározása jellemzően a nemzeti MI stratégiákban is megjelenik, amelyek az MI emberi intelligenciához való viszonyát, valamint öntanuló képességeit állítják középpontba. Így Magyarország Mesterséges Intelligencia Stratégiája például az MI-t az alábbiak szerint határozza meg, „*mint a betáplált adatok alapján önmagukat tanítani és javítani képes algoritmikus rendszerek összessége*”.[50]

c. A mesterséges intelligencia etikai alapjai és társadalmi hatásai

Ahogy az a korábban írtakból is látszik, nem létezhet az emberiséget megfelelő módon szolgáló MI megfelelő etikai alapelvek nélkül. Ezek közül az asimovi alapelvek általános érvényűnek tekinthetők – annak ellenére, hogy ezeket Asimov a robotokra, azaz az MI fizikai megtestesüléseire vonatkozóan alakította ki –,[51] azaz valamennyi MI-re általános érvénnyel kijelenthető, hogy az csak emberre nem veszélyes módon alkalmazható, mindig az ember döntésének, irányításának vagy felügyeletének alárendelten. Emellett az MI önmagát is köteles megóvni, és adott esetben fejleszteni, hogy „gazdájának” vagy tágabb értelemben a társadalomnak is a hasznára váljék. Sajnálatosan azonban ezen általános érvényű elvek sem tekinthetők minden esetben általánosan alkalmazandónak. Így például már napjainkban is beszélhetünk olyan harci drónokról, amelyek bizonyos döntéseket saját maguk lehetnek 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.[52]

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.

[50] Innovációs és Technológiai Minisztérium: Magyarország Mesterséges Intelligencia Stratégiája 2020–2030, 2020, https://ai-hungary.com/api/v1/companies/15/files/137203/view [2023.04.07.]. 6.
[51] Az asimovi alapelvek és történeti keretrendszerük kapcsán lásd fentebb a 2. pont b) alpontja kapcsán írtakat.
[52] 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/ [2023.07.14.]

Még ugyanis a gyenge MI egy-egy feladat magas szintű ellátására, egy-egy korlátozott tevékenység végzésére képes,[53] addig az erős vagy általános MI már általános intelligenciaként funkcionál, és képes az emberrel vetekedő módon gondolkodni.[54] Mindez azonban értelemszerűen beláthatatlan következményekkel járhat, hiszen egy kiszámíthatatlan természetű, az emberivel vetekedő vagy azt meghaladó szintű értelem veszélyt is jelenthet a társadalom számára, és az ember legnagyobb segítőjéből legnagyobb riválisává válhat. Ugyanakkor ezzel eltérő álláspontok is megismerhetők az MI-vel kapcsolatos irodalomban. 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.[55]

Emellett az MI fejlesztésével kapcsolatban egyéb kérdések is felmerülnek, ideértve például az MI korlátozott, jogi személyekéhez hasonló személyiséggel való felruházását, és ehhez kapcsolódó döntési kompetencia hozzárendelését. Ennek kapcsán például élénk médiavisszhangot váltott ki 2017-ben, hogy Sophia, a Hanson Robotics nevű társaság által fejlesztett robot szaúdi állampolgárságot kapott, így ezzel ő lett az első olyan robot, amelyet jogi értelemben egyfajta személyiséggel ruháztak fel.[56] Habár ezen gesztus természetesen inkább szimbolikusnak mondható, mégis egy újfajta szemléletet tükröz az MI és autonómiája kapcsán, azon felismerésnek hála, miszerint az MI már napjainkban is számos területen széleskörűnek mondható döntési kompetenciával bír (ideértve például az önvezető autókat vagy az arcfelismerő rendszereket). Az Európai Parlament a Bizottságnak szóló, a robotikára vonatkozó polgári jogi szabályokról szóló 2017. januári jelentésében is javasolta egyfajta korlátozott, „elektronikus személyiség” létrehozását azon helyzetekre, ahol a robotok önállóan döntenek vagy hasonlóan széleskörű autonómiát gyakorolnak.[57] A jelentésben foglaltakat, valamint a robotok jogalanyiságának gondolatát számos kritika érte. Egy Európai Bizottságnak címzett levélben például több mint 150 szakértő fejezte ki aggodalmát a robotok

[53] Strong AI vs. weak AI, IBM, https://www.ibm.com/topics/strong-ai [2023.05.02.]
[54] What is strong AI?, IBM [36] [2023.05.02.]
[55] Brian Christian, The Most Human Human, Anchor Books, New York, 2011. 135-136.
[56] Emily Reynolds, The agony of Sophia, the world’s first robot citizen condemned to a lifeless career in marketing, Wired, Science, 2018.06.01, https://www.wired.co.uk/article/sophia-robot-citizen-womens-rights-detriot-become-human-hanson-robotics [2023.05.03.]
[57] Jelentés a Bizottságnak szóló ajánlásokkal a robotikára vonatkozó polgári jogi ajánlásokról (2015/2103(INL)), A8-0005/2017, 2017.01.24, https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_HU.html [2023.05.03.] 19, 59(f) pont

jogalanyiságának elismerésével kapcsolatban, kiemelve többek között az MI által okozott kárral kapcsolatos felelősség erodálását.[58] A vita az MI vagy a robot esetleges jogalanyiságának, illetve jogi értelemben vett személyiségének elismerése kapcsán a fenti felvetések, kezdeményezések ellenére napjainkig eldöntetlen maradt, a jelenlegi, valamint tervezett szabályok azonban jellemzően az MI, illetve a robot szolgáltatóira, üzemeltetőire, illetve használóira telepítik a felelősséget. E tekintetben az irányadó európai uniós szabályozást alább ismertetjük.

Megemlítendő azonban, hogy amennyiben az MI-re, illetve a robotra személyként is tekintünk, úgy ezek „jogalanyként" történő meghatározása valahol az emberi és a jogi személyiség között helyezkedik el, mintegy sajátos kategóriaként. Az MI vagy a robot képességei és tevékenysége ugyanis sok esetben az emberéhez hasonlíthatók, azonban értelemszerűen nem tekinthető élőlénynek, az MI-hez vagy a robothoz továbbá a jogi személyekhez hasonló szervezettség és vagyontömeg sem társul, amely a vele szemben való felelősség érvényesíthetőségét garantálná. A technológia fejlődésével azonban egyre inkább felerősödhetnek azok a gondolatok, amelyek az MI, valamint a robotok részére jogok és felelősség rendelését követelik. Mindez valószínűleg az MI képességeinek, társadalmi jelentőségének alakulásával párhuzamosan fog megtörténni, az esetleges pozitív szabályozás azonban minden esetben csak az etikai szempontok figyelembevételével, valamint az ember és az emberi társadalom érdekeit és biztonságát szem előtt tartva foghat helyt. Kiemelendő azonban, hogy a közeljövő szabályozása vélhetően inkább az MI-t és a robotot alkalmazó, valamint felügyelő személyre telepíti majd a felelősséget, az MI-t inkább eszköznek, mint jogi értelemben vett személynek tekintve. Az MI fejlődése azonban kétségtelenül rapid módon halad, és akár számos olyan vívmánynak is a tanúi lehetünk rövid időn belül, amelyekre napjainkban még csak nem is gondolunk. Az MI elvi értelemben gondolt „személyisége" azonban álláspontunk szerint nem tekinthető egyenlőnek az emberével, azzal egyezőként pedig nem értékelhető, kizárólag ahhoz hasonlítva vagy viszonyítva, egy másodlagos személyiségként, így a jövő szabályozása sem juthat el meglátásaink szerint addig a pontig, hogy az MI-re az emberrel egyenlő entitásként tekintsen. Kiemelendő továbbá, hogy ennél sarkosabb álláspontok is megjelennek a jogirodalomban, amelyek az MI-t és a robotokat az emberiség védelmében tartanák egyfajta jogfosztott vagy „jog nélküli" kategóriában. Így

[58] Open Letter to the European Commission, Artificial Intelligence and Robotics, https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf [2023.06.11.]. 1.

például Joanna J. Bryson vonatkozó tanulmányában akként fogalmaz, és amellett érvel, hogy a robotoknak az emberek szolgáinak kell maradnia.[59]

A fentiektől eltekintve, és az MI képességeinek fejlődésére fókuszálva az utóbbi időben különösen a chatbotok, digitális asszisztensek és egyéb hasonló nagy nyelvi feldolgozáson alapuló MI-alapú megoldások területén figyelhetünk meg robbanásszerű fejlődést. Az emberekkel való társalgásra létrehozott, illetve használt chatbotok[60] azonban hosszú utat jártak be napjaink sokrétűnek mondható, magas fejlettségű alkalmazásaiig. A korábban írtak szerint az első chatbotot, ELIZA-t, 1966-ban fejlesztették ki, az MIT egyik kutatója, Joseph Weizenbaum vezetésével, egy pszichoterapeutával folytatott beszélgetés imitálása céljából.[61] Ezt követte az 1972-ben, Kenneth Kolby pszichiáter által kifejlesztett, skizofrénekkel való beszélgetésre tervezett PARRY elnevezésű alkalmazás. A két alkalmazás egyébként 1972-ben „beszélgetett" egymással, amelynek eredménye egy részben fura, illetve szellemesnek mondható „társalgás" lett, amelyben szó esett többek között a szervezett bűnözésről és a szerencsejátékról is, amely iránt PARRY különösen nagy érdeklődést mutatott.[62] Ezt követően az egyik áttörést a Richard Wallace szoftverfejlesztő által létrehozott, általánosabb célokra használható, 1995-ben megjelent chatbot, Alice jelentette,[63] amelyet később a nagy technológiai vállalatok által fejlesztett, digitális segédek követtek, ideértve például a 2010-ben, az Apple által megjelentetett SIRI, az Amazon által 2014-ben megjelentetett Alexa vagy a Microsoft által szintén 2014-ben megjelentetett Cortana elnevezésű alkalmazást. Ezek a digitális segédek 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 társalgásokat is folytathattak az adott alkalmazással.

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 hétköznapi társalgáson túl számos, komplexebbnek tekinthető feladat

[59] Joanna J. Bryson, Robots Should Be Slaves, 2010.03.24, DOI:10.1075/nlp.8.11bry [2023.09.06.]
[60] What is a chatbot? Oracle, https://www.oracle.com/ie/chatbots/what-is-a-chatbot/ [2023.04.23.]
[61] ELIZA [39]
[62] 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 [2023.04.23.], Network Working Group, V. Cerf, PARRY Encounters the DOCTOR, 1973.01.21, https://datatracker.ietf.org/doc/html/rfc439 [2023.04.23.]
[63] Alice chatbot wins for third time, BBC News, last updated: 2004.09.20, http://news.bbc.co.uk/2/hi/technology/3672424.stm [2023.04.23.]

elvégzésére is képes, ideértve – többek között – cikkek vagy elbeszélések írását, programozási vagy fordítási feladatok elvégzését. 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.[64]

Természetesen a chatbot alkalmazásokon túl számos egyéb területen is forradalmivá vált az MI, ideértve például a képszerkesztést. A szintén OpenAI által fejlesztett DALL-E vagy a független Midjourney, Inc. kutatószervezet által létrehozott, Midjourney elnevezésű alkalmazás[65] képes például művészi vagy akár fotórealisztikus képek létrehozására is. Léteznek ugyanakkor MI-alapú megoldások kifejezetten irodalmi művek vagy zenei alkotások létrehozására is, annak újragondolására késztetve minket, hogyan is viszonyulunk a művészet és az alkotás emberi jellegéhez. Olyan is előfordult már ugyanis, hogy egy kifejezetten művészi versenyt MI alkalmazás által alkotott alkotás nyert meg. Így például a német művész, Boris Eldagsen 2023. áprilisában jelentette be, hogy nem veszi át a Sony fényképészeti világversenyen nyert díját, mivel a díjnyertes művet egy MI alkotta, az indulást pedig egyfajta provokációnak szánta.[66]

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 állítja az emberiséget, egyben megkövetelve a nagyvállalatoktól, a nemzeti kormányoktól, valamint a társadalom egészétől egyfajta társadalmi megállapodás vagy konszenzus létrehozását 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.[67] Értelemszerűen azonban egy szélesebb, az ipari szereplőkön és szolgáltatók körén túlmutató társadalmi konszenzusnak is meg kell születnie az MI alkalmazásának korlátairól, szabályairól, amely kapcsán azonban napjainkban még inkább eltérő nemzeti vagy regionális meglátásokról, irányokról beszélhetünk.

---

[64] Böcskei Balázs, Német Szilvi, Toxikus technokultúrák és digitális politika. Érzelmek, mémek, adatpolitika és figyelem az interneten, Napvilág Kiadó – TK PTI, 2021. 151.
[65] Lásd: Midjourney, https://www.midjourney.com/ [2023.05.06.]
[66] Jamie Grierson, Photographer admits prize-winning image was AI-generated, The Guardian, Culture, 2023.04.17., https://www.theguardian.com/technology/2023/apr/17/photographer-admits-prize-winning-image-was-ai-generated [2023.05.06.]
[67] Democratizing AI: Satya Nadella on AI vision and societal impact at DLD, Microsoft, 2017.01.17, https://news.microsoft.com/europe/2017/01/17/democratizing-ai-satya-nadella-shares-vision-at-dld/ [2023.04.07.]

Bizonyos esetekben a fejlesztések korlátozásával, felfüggesztésével kapcsolatos hangok is felerősödni látszanak, amelyek a társadalom védelme szempontjából elengedhetetlennek tekintik az MI-alapú fejlesztések területén való „lassítást". A közelmúltban például számos szakértő, illetve vezető személyiség, például a techmilliárdos, Elon Musk, írt alá egy levelet, amely az MI fejlesztésekkel kapcsolatos lehetséges veszélyekre való reagálásként GPT-4 elnevezésű alkalmazásnál fejlettebb MI-alapú megoldások fejlesztésének 6 hónapos felfüggesztésére szólított fel.[68] Mindez azonban vélhetőleg nem fog a fejlődés megakasztásához vezetni, ugyanis az e mögötti anyagi és egyéb érdekek, valamint a felfedezés iránti emberi vágy látszólag az MI területén sem ismer korlátokat, egy esetleges „leállás" pedig nem biztos, hogy a technológia fejlődésével járó veszélyekre adott arányos válasz lenne.

A fentiek kapcsán álláspontunk szerint az MI-alapú fejlesztésekkel kapcsolatos korlátokra és szabályokra szükség van, általános fejlesztési korlátozás vagy tilalom bevezetése azonban némely területeken aggályos lehet (ideértve például az egészségügyi kutatások területét), illetve az MI fejlődésével járó pozitív és a negatív hatások egységes visszafogásához vezethet. 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" hatósági reakció, valamint a rövid-távú eredményeket előnyben részesítő szabályozás 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 lehetnek, ezek ugyanis biztonságos keretet nyújtanak egy-egy innovatív megoldás kipróbálásához, mielőtt azok az adott piacon nyíltan kerülnének alkalmazásra. Ennek kapcsán jó példának tekinthető az Európai Bizottság által, az ún. elosztott főkönyvi technológiák (angolul: „*Distributed Ledger Technologies*", röviden: „*DLT*") kapcsán 2023-ban bevezetett sandbox.[69]

[68] Pause Giant AI Experiments: An Open Letter, https://futureoflife.org/open-letter/pause-giant-ai-experiments/ [2023.06.11.]
[69] Launch of the European Blockchain Regulatory Sandbox, 2023.02.14, https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox [2023.06.11.]

d. Szabályozható-e a mesterséges intelligencia, valamint a digitalizáció vívmányai a technológiai és a társadalmi fejlődés megakasztása nélkül?

Az MI szabályozása kapcsán – az ennek szükségességét alátámasztó érveken túl – gyakran merül fel a technológiai és társadalmi fejlődés megakasztásától 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.

A fentiekre tekintettel a tanulmány jelen pontjában az MI-vel kapcsolatos főbb lehetőségeket és veszélyeket tárgyalom, ideértve az MI-vel kapcsolatos főbb szabályozási irányvonalakat. Emellett ugyancsak kitérek arra, hogy mely személyek, illetve szervezetek lehetnek hivatottak arra, hogy az MI-t szabályozzák, illetve milyen körben, milyen szabályozási szinteken. A fentieken túl kitérek arra is, hogy milyen alapelveket szükséges a szabályozóknak figyelembe venniük az MI fejlesztésének és alkalmazásának szabályozása során. Emellett szintén kitérek a szabályozással kapcsolatos megközelítésekre, és az egyes szabályozási módokra is.

i. A szabályozással kapcsolatos veszélyek és lehetőségek, a főbb szabályozási irányvonalak

A fentebb előadottak tükrében látható, hogy a digitalizáció vívmányai, és különösen az MI megfelelő szabályozási keretrendszert igényelnek ahhoz, hogy az emberiséget szolgálva fejlődhessenek, azonban a szabályozatlanságból eredő kockázatok és negatív hatások nélkül. 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.

Az MI fejlődésével és elterjedésével kapcsolatos pozitív hatásokat nehéz vitatni, ezek a társadalom, illetve a gazdaság szinte valamennyi területén, illetve számos szintjén megmutatkoznak. A chatbotok és digitális asszisztensek segítségével könnyebbé válhat az ügyintézés, valamint egyes egyszerűbbnek tekinthető hétköznapi feladatok elvégzése, míg például a szociális és egészségügyi robotok sok szempontból javíthatnak az egészségügyi és

szociális ellátáson, és könnyebbé tehetik számos ember életét. A fentieken túl számos egyéb 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 az MI, és az MI által feldolgozott jelentős adatmennyiség emellett önmagukban is katalizáló hatással bírnak a tudományos fejlődésre, illetve ahhoz jelentős hozzájárulást nyújtanak.[70]

A fenti innovációk, új technológiák, megoldások alkalmazása azonban 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 utóbbi időkben különösen az MI-vel kapcsolatos félelmek kaptak hangot, amelyek a leginkább az MI öntudatra ébredésére, valamint az emberi civilizációt veszélyeztető beláthatatlan fejlődésére és irányíthatatlanságára fókuszálnak. A 2018-ban elhunyt, neves angol matematikus, Stephen Hawking például már a halála előtt is az MI kontrolállhatatlan fejlődésével kapcsolatos veszélyekre, és annak az emberiségre gyakorolt végzetes hatásaira hívta fel a figyelmet.[71] Természetesen, habár a fenti kritikák megfelelő racionalitással kezelendők, az azonban kétségtelenül vitathatatlan, hogy az MI megfelelő emberi felügyelet nélküli fejlődése komoly kockázatokkal járhat. Például, képzeljük csak el, mi történne, ha az MI venné át egyik napról a másikra egy egész város, vagy akárcsak az autónk vezetését. Az MI-vel kapcsolatos biztonsági kockázatok jelentőségét jól jelzi, hogy az ENSZ Biztonsági Tanácsa nemrégiben története során először tartott ülést az MI nemzetközi békére és biztonságra jelentett veszélyeinek témájában.[72]

Érthető módon a fenti veszélyekre, valamint az azokkal kapcsolatos aggodalmakra tekintettel nyertek nagyobb teret a közelmúltban a fentebb említett kritikák is, valamint a fejlesztések korlátozásával vagy átláthatóbbá tételével kapcsolatos törekvések, és a nemzetek, illetve a nagyvállalatok közötti nagyobb fokú együttműködés iránti követelések. Ennek kapcsán Sam Altman, a ChatGPT megoldást kifejlesztő OpenAI intézet vezető tisztségviselője például nemrég nemzetközi együttműködésre és közös szabályozásra szólított fel az MI alapú

[70] Mark Owen, Maria Luchian, Following the AI path, Intellectual property magazine, 2044-7175. (September 2020). 15-16. 15.
[71] Rory Cellan-Jones, Stephen Hawking warns artificial intelligence could end mankind, BBC News, 2014.12.02, https://www.bbc.com/news/technology-30290540 [2023.06.25.]
[72] Edith M. Lederer, UN council to hold first meeting on potential threats of artificial intelligence to global peace, AP News, Technology, 2023.07.03, https://apnews.com/article/artificial-intelligence-un-security-council-meeting-uk-f7fb6d8f8a261a9d9b23ca463ee29d3d [2023.07.14]

megoldások fejlesztése területén.[73] Mindazonáltal óvatos, a félelmek enyhítését célzó megjegyzések is egyre inkább hangzanak el az MI kapcsán, főként a technológia fejlesztésében különösen érdekelt nagyvállalatok és egyes bizakodó szakértők részéről. Például a Microsoft technológiai nagyvállalat MI részlegének vezetője, Eric Boyd a Sky News-nak 2023-ban adott interjújában kifejezetten az MI-ben rejlő lehetőségeket, pozitív társadalmi és gazdasági folyamatokat hangsúlyozta, valamint azon álláspontját is kifejtette, miszerint az MI jelenlegi fejlettségi szintjén nem jelent veszélyt az emberiségre.[74]

Természetesen azonban az MI felügyeletével, a fejlesztések esetleges korlátozásával vagy mederbe terelésével, az érdekelt felek közti együttműködés erősítésével kapcsolatos törekvések előtt számos akadály áll. Ilyennek tekinthető például a technológiai vállalatok és a tudományos kutatóintézetek közti piaci, illetve tudományos verseny, továbbá a mindennapok megkönnyítése iránti lankadatlan fogyasztói és társadalmi igény, valamint végső soron az emberi felfedezések fő hajtóereje, az emberi kíváncsiság is. Könnyen lehet, hogy az MI hétköznapi életünk olyan szerves részévé válik majd, mint az internet, a számítógép, vagy a világunk működését megkönnyítő elektronikus adatfeldolgozás-, illetve adatátvitel.[75] Ebben a tekintetben az MI nehezen fogható fel egy egységesen szabályozható technológiaként, ugyanis mind az MI-ben rejlő lehetőségek kihasználásával kapcsolatos érdekek, mind az MI hallatlan sokoldalúsága és emberarcú jellege is a korlátozások, valamint a túlzott szabályozói „mederbe terelés” ellen hatnak.

A fentiek tükrében így az is vitathatatlan, hogy a túlságosan szigorú vagy egyéb okból nem megfelelő szabályozás is veszélyekkel járhat, különösen a tudományos fejlődés megakasztásával, valamint a társadalmi, gazdasági folyamatok megtörésével. Például: bizonyos MI-alapú megoldások betiltása egyben azokat a problémákat is felerősítheti, amelyek orvoslására az adott MI-rendszer tilalom által érintett felhasználására eleve sor került. Hasonló utat járt be az arcfelismerő rendszerek megítélése. Ezek felhasználását ugyanis számos területen mind a jogalkotó, mind a társadalom egy jelentős része alkotmányos szempontból sérelmesnek tartja (ideértve például a demokratikus működést veszélyeztető teljes megfigyeléstől való

[73] 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 [2023.06.25.]
[74] 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 [2023.07.14.]
[75] Nagy Zoltán András, Bűncselekmények számítógépes környezetben, Ad Librum, Budapest, 2009. 6.

félelmet vagy a hibás vagy diszkriminatív azonosítási gyakorlatból származó kockázatokat), ugyanakkor az is vitathatatlan, hogy különösen jelentős bűncselekmények (például: terrorcselekmények) megakadályozása vagy az ilyen cselekmények elkövetőinek kézre kerítése kapcsán a technológia jelentős segítséget nyújthat, katasztrófákat előzhet meg, és így emberéletek megmentéséhez vezethet. A technológia ugyancsak segítséget nyújthat például eltűnt személyek megtalálásában vagy veszélyes vagy nehezen átlátható területek átfésülésében, mentőakciók lefolytatásában. Így az arcfelismerő technológia alkalmazásával kapcsolatos teljes tilalom is éppúgy ártalmas lehet, mint az általános tilalom bevezetése. Erre tekintettel alkalmasabb lehet csak a kiemelten kockázatos felhasználási módok tekintetében érvényesülő (rész)tilalmak, illetve arányos korlátozások bevezetése (például: magánszféra védelme érdekében bizonyos helyeken való alkalmazás tilalma) vagy a társadalom, illetve az érintettek jogait és érdekeit védő követelmények felállítása (például: a technológia tesztelésével, felülvizsgálatával kapcsolatos követelmények).[76]

Így a fentebb írtakkal összhangban, az MI és a digitalizáció vívmányai tekintetében olyan szabályozási megközelítés lehet megfelelőnek tekinthető, amely arányosan reflektál az adott megoldás által támasztott kockázatokra, az érintettek érdekeinek, az adott terület sajátosságainak, valamint a megoldás alkalmazásával járó társadalmi és gazdasági hatások és folyamatok figyelembevételével. Mindez értelemszerűen nem feltétlenül kell, hogy teljesen egységes szabályozást eredményezzen, az adott szabályozásnak ugyanis a társadalmi és kulturális szempontokat és sajátosságokat, valamint az adott közösségek érdekeit is figyelembe kell vennie. Egyes megoldások tekintetében, valamint egyes területeken így feltételezhetően egységesebbnek tekinthető, vagy jellemzően gazdasági szempontokat figyelembe vevő szabályozás kialakulása, míg más területeken kulturális szempontból jóval sokrétűbb szabályozás kialakulása várható, az egyes országok, régiók, vagy akár szektorok tekintetében is. Az MI szenzitívebbnek tekinthető területeken való alkalmazása esetén például erőteljesebb szabályozás várható a demokratikus hagyományokkal bíró országokban, mint például az eltérő államberendezkedéssel bírókban.

Habár az országok jelentős része már dolgozik valamilyen szabályozási megközelítésen az MI kapcsán, vagy ezen koncepciók átültetésének már neki is fogott, e tekintetben is szembetűnőnek tetszik az európai és az amerikai szabályozási megközelítések különbsége. Az európai

[76] Az arcfelismerő rendszerek alkalmazásával kapcsolatos szabályozás és egyes egyéb szempontok kapcsán alább, a vonatkozó fejezetben írunk.

szabályozás jellemzően az általános megközelítésből indul ki, így egy általános MI jogszabályban gondolkodik, amely az MI fejlesztésének, alkalmazásának főbb szabályait és a gyártók, alkalmazók főbb kötelezettségeit tartalmazza, míg az amerikai szabályozás inkább szektorális megközelítést alkalmaz, és az egyes szakterületek vagy szempontok tükrében szabályozza az MI-t. E körben szintén kiemelendők az egyes tagállamok szabályozási koncepciói, a tagállami szabályok ugyanis várhatóan a jövőben is számos lényeges kérdésben lesznek meghatározók. Az EU tagállamok esetén ez értelemszerűen csak az európai uniós szabályozással összhangban, arra tekintettel történhet, míg az Egyesült Államokban az egyes államok alkotmányos jogainak keretein belül, valamint a szövetségi szabályozás által lehetővé tett körben.

ii. Ki szabályozza az MI-t és milyen szabályozási szinteken?

A fentebb írtakkal összhangban napjainkban az is kérdéseket vet fel, hogy pontosan mely szervezet vagy szervezetek hivatottak szabályozni az MI-t, és milyen szinteken? Így mennyire szükséges nemzetközi konszenzus elérése egy-egy kérdésben, illetve milyen döntési kompetenciával kell, hogy bírjanak az egyes államok, szakmai szervezetek vagy nagyvállalatok? Problémát jelent-e továbbá, ha az MI fejlődését egy-egy területen tisztán a piacra bízzuk? Ezek mind-mind olyan kérdések, amelyek jelentős mértékben foglalkoztatják a nemzetközi és a nemzeti szabályozókat, valamint a különböző szakmai szervezeteket és gazdasági szereplőket is.

A nemzetközi szabályozás tekintetében kiemelt jelentőséggel bírnak az alábbi táblázatban felsorolt kezdeményezések, illetve jogszabálytervezetek:

Szabályozó	Kezdeményezés vagy szabályozás	Jelentőség[77]
Az Együttműködésben résztvevő tagállamok, valamint az EU	Globális Együttműködés az MI Területén (angolul: „*Global Partnership on*	Az együttműködéshez eddig 29 ország csatlakozott, ideértve

[77] Az egyes szabályozási kezdeményezések azonosítása kapcsán alapul vettük az alábbi cikkben foglaltakat: Melissa Heikkilä, Our quick guide to the 6 ways we can regulate AI, MIT Technology Review, 2023.05.22, https://www.technologyreview.com/2023/05/22/1073482/our-quick-guide-to-the-6-ways-we-can-regulate-ai/ [2023.06.25.]

	Artificial Intelligence"; „*GPAI*")[78]	többek között az Egyesült Államokat, Kanadát, az Európai Uniót, Németországot, Franciaországot, valamint több egyéb európai, afrikai, ázsiai, valamint óceániai országot (például: Japán, India, Ausztrália, stb.).
OECD	MI Alapelvek[79]	A fenti alapelvek általános jelleggel határoznak meg követelményeket az MI megoldásokkal kapcsolatban, amely az OECD jelentőségére tekintettel kiemelt hivatkozási pontként szolgál az MI szabályozás kapcsán.
Európa Tanács	Egyezmény a Mesterséges Intelligenciáról, az Emberi Jogokról, a Demokráciáról és a Jog Uralmáról („**ET Egyezmény**")[80]	Az ET Egyezmény az Európa Tanács emberi jogi tevékenysége okán jelentős hivatkozási pontnak tekinthető az MI szabályozás kapcsán.
EU	Mesterséges Intelligenciáról Szóló	Átfogó MI szabályozást megvalósító jogszabály, amely az egyes megoldások kockázati

[78] GPAI, https://gpai.ai/about/ [2023.07.09.]
[79] OECD, AI Principles, https://oecd.ai/en/ai-principles [2023.06.25.]
[80] 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 [2023.06.25.]

	Jogszabály tervezete („**MI Rendelet Tervezet**”)[81]	tényezőinek megfelelően rögzít különböző tilalmakat és követelményeket.

A GPAI a fentiekkel, valamint az OECD MI értékalapú irányelveivel összhangban a megbízható MI-vel való gazdálkodás kapcsán bizonyos alapelveket, valamint a megbízható MI-vel kapcsolatos nemzeti politikák és nemzetközi együttműködés területén is szempontokat határoz meg.

E körben a GPAI a megbízható MI-vel való gazdálkodás kapcsán az alábbi alapelveket határozza meg:

- inkluzív növekedés, fenntartható fejlődés és jólét,
- ember-központú értékek és tisztesség,
- átláthatóság és megmagyarázhatóság,
- megbízhatóság, biztonság és védelem,
- elszámoltathatóság.[82]

Emellett a GPAI a megbízható MI-vel kapcsolatos nemzeti politikák és nemzetközi együttműködés területén az alábbi szempontokat határozza meg:

- az MI kutatásokba való befektetés és fejlesztés,
- digitális ökoszisztéma kialakítása az MI számára,
- szabályozói környezet kialakítása és lehetővé tétele az MI számára,
- humánerőforrás fejlesztés, valamint a munkaerőpiaci átalakulásra való felkészülés,
- a megbízható MI kapcsán való nemzetközi együttműködés.[83]

Ahogy az a fentiekből is látható, a GPAI tehát a megbízható MI alkalmazása, valamint az azzal való gazdálkodás kapcsán kiemelt jelentőséget tulajdonít az emberközpontúságnak, valamint az átlátható, megbízható és biztonságos MI alkalmazásnak, amelyet a fenntartható fejlődés

[81] 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, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0206 [2023.06.25.]
[82] GPAI [78]
[83] Uo.

keretein belül, az emberiség, illetve az emberi közösségek jóléte érdekében alkalmaznak, elszámoltatható módon. Emellett a GPAI a vonatkozó szabályozás kapcsán kiemelt jelentőséget tulajdonít a kutatások ösztönzésének, megfelelő digitális ökoszisztéma kialakításának, amely serkenti a versenyt, valamint a társadalmi és gazdasági fejlődést, illetve megfelelő és áttekinthető szabályozói környezet kialakítását, az MI szabályozásával kapcsolatos nemzetközi együttműködést követel meg. Hangsúlyozza továbbá a humánerőforrás képzést, tekintettel arra, hogy az MI-re nem az embert felváltó, hanem azt segítő technológiaként tekint.

Ugyancsak jelentős kezdeményezésnek tekinthetők az OECD 2019. májusában elfogadott MI Alapelvei, 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.[84]

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.

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

- befektetés az MI-alapú kutatás- 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.[85]

[84] OECD, MI Alapelvek, 7-8.
[85] OECD, MI Alapelvek, 8-9.

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, valamint a fejlődés megakasztásához vezethet.

Az ET Egyezmény 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 hatóság 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 lehetőség szerinti elkerülését; emellett az ET egyezmény hangsúlyozza az MI demokratikus intézmények általi, a jog uralmára tekintettel való alkalmazásának fontosságát, az alkalmazás során, illetve azt megelőzően a szükségesség, arányosság, valamint a lehetséges kockázatok felmérését, ezzel kapcsolatban megfelelő intézkedések megtételét.[86]

Az MI termékértékesítés, valamint szolgáltatásnyújtás során történő felhasználása kapcsán az ET Egyezmény szintén hangsúlyozza ezek emberi jogok, valamint a demokratikus társadalmak elvárásaira, vonatkozó jogszabályi követelményekre tekintettel történő végzését, az emberi jogok és alapvető szabadságok, valamint a demokratikus társadalmi működés megsértésének

[86] ET Egyezmény, 5-6.

kerülését. 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.[87]

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,
- az átláthatóság és a felülvizsgálat elvét,
- a biztonság elvét,
- a biztonságos innováció elvét.[88]

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.[89] 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 információt nyújtó vagy döntést hozó MI rendszerek esetén, a kapcsolódó emberi kommunikációt, valamint hatékony hozzájutást a vonatkozó garanciákhoz és lehetőségekhez.[90]

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

[87] ET Egyezmény, 6.
[88] ET Egyezmény, 6-7.
[89] ET Egyezmény, 7.
[90] ET Egyezmény, 8.

társadalom működésével, valamint a jog uralmának betartásával, az ezekkel kapcsolatos esetleges károk és veszélyek elkerülésével kapcsolatban.[91]

Mindemellett az ET Egyezmény szintén hangsúlyozza az MI-vel, a kapcsolódó kockázatokkal és hatásokkal kapcsolatos képzések fontosságát,[92] valamint a nemzetközi együttműködést és a nemzeti hatóságok megfelelő és demokratikus eljárását, erőforrásokkal való ellátását.[93]

A fentebb írtakkal összhangban álláspontunk szerint kijelenthető, hogy a nemzeti MI szabályozásnak elsődlegesen nemzetközi szabályozási keretrendszeren, illetve a nemzetközi közösség által is elismert etikai és szabályozási alapelveken kell nyugodnia. Természetesen mindez nem jelenti azt, hogy a nemzeti vagy regionális MI szabályozások ne tükrözhetnének sajátos meglátásokat vagy irányzatokat, illetve ne lenne szükség arra, hogy ezen szabályozások a helyi kulturális, vallási, szociális és gazdasági szempontokat figyelembe vegyék. Sőt, ennek épp az ellenkezője jelenthető ki, hiszen a helyi szabályozásnak – 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.

A fentieken túl azonban az is kijelenthető, hogy az MI szabályozás – sem nemzetközi, regionális vagy nemzeti szinten – nem képzelhető el az érintett közösségek és gazdasági, szakmai szereplők bevonása, a velük történő konzultáció nélkül. Erre jó példának tekinthetők a fenti technológiai vállalatok állásfoglalásai és egyéb kommunikációi, amelyek – számos esetben a nemzetközi vagy regionális kommunikációkkal, etikai állásfoglalásokkal és stratégiákkal összhangban – jelenítik meg az adott szektor szakmai és gazdasági szereplőinek álláspontját, érdekeit, vízióit, valamint az általuk vallott értékeket.

Érthető módon az MI szabályozás tekintetében viszont a regionális szempontokkal és szabályozási környezettel összhangban álló nemzeti szabályozásnak kell középpontban állnia, hiszen így biztosítható, hogy az MI fejlesztését és alkalmazását (ideértve különösen a kockázatosnak ítélt alkalmazási módokat) az adott szektor érdekein felül, illetve azon kívül álló független szerv felügyelje.

[91] ET Egyezmény, 9.
[92] Uo.
[93] ET Egyezmény, 9-10.

A fentiek tükrében elképzelhető azonban, hogy egy-egy szektorban társ- vagy önszabályozás alakul ki, így az állami szervek helyett vagy mellett az adott szakmai felügyeleti szervek, szakmai fórumok vagy egyéb szereplők kapnak majd teret az MI szabályozása kapcsán. Ez különösen az olyan sajátos szakterületeken tűnik lehetségesnek, ahol az ön- és társszabályozás egyébként is erősnek mondható, és jelentős történelmi múltra tekint vissza. Így a jövőben lehetséges majd, hogy az ügyvédi vagy az orvosi kamara írjon elő az ügyvédek vagy az orvosok számára bizonyos szakmai szabályokat az MI-rendszerek ügyvédi vagy orvosi alkalmazása során, az irányadó regionális és nemzeti szabályok mellett. Elképzelhetőnek tűnik továbbá az is, hogy a sajtó és a médiaipar területén az illetékes hatóság mellett az adott szakmai szervezetnek is beleszólása lehessen abba, hogy mely területen tekinthető etikusnak a robotújságírás, és milyen szakmai szabályoknak szükséges vagy javasolt megfelelnie.

iii. Milyen alapelveket kell figyelembe vennünk az MI szabályozása során?

Az MI szabályozás során elsődlegesen azon alapelveket szükséges meghatározni, amelyek a teljes szabályozáson áthatva iránymutatásként és egyben szilárd követelményrendszerként szolgálnak a szabályozás által érintett személyek és szervezetek számára. Számos esetben az MI szabályozás alapelvi gyökereit az emberi jogi alapelvek között kell keresnünk, tekintettel arra, hogy az MI szabályozás egyetemesnek tekinthető célja az emberiség előbbre vitele, valamint az egyén és az emberi közösségek védelme a technológia nem megfelelő alkalmazásából származó hátrányoktól.

A fentiek kapcsán példaként említhető az Emberi Jogok Európai Egyezménye („**EJEE**”),[94] amely alapvetően foglalja össze és tükrözi az alapvető emberi jogokat. Ezen jogok jellemzően az MI alkalmazása tekintetben is jelentőséggel bírhatnak, ideértve például az élethez való jogot[95] vagy a magán- és családi élet tiszteletben tartásához való jogot.[96] Értelemszerűen azonban még tisztázandó, hogy ezen jogok védelme kapcsán pontosan milyen szempontoknak kell érvényesülniük az MI egyes alkalmazásai tekintetében, illetve milyen intézkedéseket

[94] A 11., 14 és 15. Kiegészítő Jegyzőkönyv által módosított Emberi Jogok Európai Egyezménye, valamint az 1., 4., 6., 7., 12., 13. és 16. Kiegészítő Jegyzőkönyv, https://www.echr.coe.int/documents/d/echr/Convention_HUN [2023.07.16.]
[95] EJEE 2. cikk
[96] EJEE 8. cikk

szükséges meghozni az emberi jogok védelme érdekében az egyes szakterületeken. Ezen szabályozási kihívások, illetve kérdések megválaszolása a jövő feladata.

A fentiekkel összhangban tehát az MI szabályozásnak mindenképpen emberarcúnak kell maradnia, és az emberiség, az emberi közösségek érdekeivel összhangban kell állnia. E körben segítséget nyújthatnak az irodalomból már ismert asimov-i alapelvek, amelyek hallatlan humánummal ragadják meg az ember és a gép viszonyát. Ezek tükrében érdemes lehet végig gondolni, hogy bizonyos alapelvek alkalmazhatók-e (majd) kizárólag a robotokra (tehát az MI fizikai megtestesülésére), a technológia jelenlegi állása mellett azonban jellemzően a nemzetközi és nemzeti alapelvi meghatározások az MI-vel szembeni általános követelményekből indulnak ki, amelyek mind a robotok, mind a fizikai megjelenés nélküli algoritmusok esetén irányadók lehetnek.[97]

Magyarország Mesterséges Intelligencia Stratégiája nem határoz meg külön alapelveket, és a nemzetközi, valamint az európai szabályozás keretrendszeréből, az ennek keretén belül lefektetett alapelvekből indul ki.[98] 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:

- 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.[99]

Mindemellett a dokumentum a magyar MI stratégia célrendszerét akként foglalja össze, miszerint „*Együtt tanuljuk, hatékonyan fejlesztjük és használjuk az MI technológiákat,*

[97] Ennek kapcsán lásd például az általunk az európai uniós MI szabályozás kapcsán alább ismertetett meghatározásokat.
[98] Magyarország Mesterséges Intelligencia Stratégiája 2020-2030, 2020. május, https://ai-hungary.com/api/v1/companies/15/files/137203/view [2023.07.16.]
[99] Magyarország Mesterséges Intelligencia Stratégiája [98]. 17-18.

felelősen, keretezetten, globális partnerként, a hétköznapok szolgálatában".[100] Mindezen megállapítás és elhatározás kétségtelenül reális és eredményes célkitűzést ad az MI-vel való felelős stratégiai tervezés számára.

A fentiek mellett természetesen szinte minden ország közzétett már MI-vel és az MI szabályozással kapcsolatos stratégiát, iránymutatást, illetve etikai témájú nyilatkozatot vagy más hasonló dokumentumot. E körben érdekességnek tekinthető, hogy maga a Vatikán is meghatározta az MI etikai alapelveit „Róma Felhívása az MI Etika Kapcsán" című, 2020. február 28-án kelt anyagában. E körben az alábbi alapelvek kerülnek meghatározásra:

- átláthatóság,
- befogadás,
- felelősség,
- pártatlanság,
- megbízhatóság,
- biztonság és adatvédelem.[101]

Mint a fentebb, illetve a jelen pontban alább írtak szerint is látszik, a Vatikán tehát sok szempontból az egyéb államokhoz, valamint az iparági szereplőkhöz hasonló módon, illetve szempontok szerint határozta meg az MI etikai alapelveit, ideértve különösen az MI átláthatóságával, megbízhatóságával és az érintettek érdekeinek figyelembevételével kapcsolatos szempontokat.

Az Egyesült Államokban az amerikai MI szabályozással kapcsolatos alapelveket a 2022-ben megjelent „*Blueprint for an AI Bill of Rights*" elnevezésű dokumentum („**Blueprint**") foglalja össze. Ezen alapelvek közé az alábbiak tartoznak:

- biztonságos és hatékony rendszerek,
- algoritmikus diszkrimináció elleni védelem,
- adatvédelem,
- figyelemfelhívás és magyarázat,

[100] Magyarország Mesterséges Intelligencia Stratégiája [98]. 18.
[101] Rome Call for AI Ethics, 2020.02.28, https://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rc_pont-acd_life_doc_20202228_rome-call-for-ai-ethics_en.pdf [2023.07.09.]. 6-7.

- emberi alternatívák, megfontolás és megoldás.[102]

A fentiekre tekintettel a dokumentum hangsúlyozza a megbízhatatlan és nem hatékony rendszerekkel szembeni védelmet, e körbe értve a nem megfelelő vagy nem releváns adatok felhasználással szembeni védelmet is.[103] 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.[104] A dokumentum kiemeli továbbá az amerikaiak jogait a visszaélésszerű adatkezelési gyakorlatoktól beépített védelmi lehetőségek által, valamint hangsúlyozza az érintettek jogát az adataik felhasználásával kapcsolatos rendelkezésről.[105] 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.[106] 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.[107]

A fentiek szerint a dokumentum több esetben is az európai adatvédelmi szabályozás 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.

[102] 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 [2023.07.16.], 5-7.
[103] Blueprint for an AI Bill of Rights [102]. 5.
[104] Uo.
[105] Blueprint for an AI Bill of Rights [102]. 6.
[106] Uo.
[107] Blueprint for an AI Bill of Rights [102]. 7.

Az állami szereplők, valamint a nemzetközi szervezetek MI stratégiái, etikai szempontjai mellett szükségesnek látszik szót ejteni a technológiai szektor MI szabályozással, valamint etikai irányelvekkel kapcsolatos szempontjairól, tekintettel arra, hogy az iparági szereplők a piaci meglátásokat és a szabályozás gyakorlati alkalmazásával kapcsolatos egyes szempontokat sok esetben jelentős saját tapasztalatokra építve tudják megjeleníteni. Ezen alapelvek és szempontok azonban – mint azt az alábbiak szerint is látni fogjuk – az esetek döntő többségében a demokratikus államok és nemzetközi szervezetek alapvetéseivel és meglátásaival egyeznek, illetve azokkal összhangba hozhatók.

Az amerikai technológiai vállalatok 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,[108] amely a ChatGPT-hez hasonlóan, általános segítő alkalmazásként szolgál.

A Google az MI kapcsán több alapelvet is meghatározott, e körbe értve az MI alapú alkalmazások céljait, illetve olyan alkalmazásokat, amelyek megalkotását, illetve használatát egyáltalán nem célozza. Így a Google az MI alapú alkalmazások kapcsán az alábbi célokat határozta meg:

- szociális hasznosság,
- az igazságtalan elfogultság elkerülése,
- biztonságosként építve és tesztelve,
- elszámoltathatónak lenni az emberek felé,
- beépített adatvédelmi alapelvek,
- magas szintű tudományos színvonal fenntartása,
- a fenti alapelveknek megfelelő használatra való elérhetővé tétel.[109]

A Google továbbá azon MI alapú alkalmazásokat is meghatározta, amelyeket nem készül sem fejleszteni, sem alkalmazni, ideértve

- olyan technológiákat, amelyek általában véve károkat okoznak. Ha jelentős esély van a károkozásra, az adott technológia fejlesztésére vagy alkalmazására csak akkor kerül sor, ha az előnyök jelentősen meghaladják a károkat, amelyeket megfelelő intézkedések révén mérsékelnek,

[108] Google, Bard Experiment, https://bard.google.com/?hl=en [2023.07.11.]
[109] Google AI, Our Principles, https://ai.google/responsibility/principles/ [2023.06.30.]

- fegyverek vagy olyan technológiák gyártását, amelyek elsődleges célja, hogy másoknak sérülést okozzanak, vagy ezt közvetlenül előmozdítsák,
- olyan technológiákat, amelyek megfigyelés céljára gyűjtenek vagy használnak fel információkat nemzetközileg elfogadott normák megsértésével,
- olyan technológiákat, amelyek célja a nemzetközi jog és az emberi jogok széleskörben elfogadott alapeszméinek megsértése.[110]

A fentiek alapján 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. Érdekesség, hogy a Google ugyancsak meghatároz olyan célokat vagy alkalmazási módokat, amelyek érdekében MI fejlesztést nem végez, illetve MI alapú megoldásokat nem alkalmaz (például: a fentiek szerinti hadászati, megfigyelési célokat). Ezen meghatározás mindenképpen példamutatónak tekintendő.

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*")[111] jó gyakorlatok, hipotetikus 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.[112] Mindemellett a fenti dokumentum hangsúlyozza az MI munkafolyamata kapcsán az emberi részvétel szükségességével kapcsolatos helyzetek pontosítását, valamint az emberi felülvizsgálattal kapcsolatos különböző megközelítések, helyzetek felmérését, felelősséggel kapcsolatos szabályozás, szektorspecifikus szempontok, kivételek és felelősségkorlátozás, valamint biztosítási lehetőségek számbavételét.[113]

[110] Uo.
[111] 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 [2023.07.04.]
[112] Google, Perspectives on Issues in AI Governance, https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf [2023.07.04.]. 5.
[113] Uo.

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.[114]

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 megfelelőségi referenciaértékek pragmatikusak legyenek, és az alkalmazás tágabb környezetére reagáljanak,
- a megbízhatóság priorizálása az elvárások körülményekre tekintettel való meghatározásával,
- az emberi felülvizsgálatra való túlzott támaszkodással kapcsolatos óvatosság az MI-vel kapcsolatos problémák kezelése területén.[115]

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

[114] Google, Recommendations for Regulating AI, https://ai.google/static/documents/recommendations-for-regulating-ai.pdf [2023.07.09.]. 2-5.
[115] Google, Recommendations for Regulating AI [114]. 6-16.

diszkriminációval szemben felszólalva –, és ugyancsak hangsúlyozza az átláthatóság fontosságát, amely az európai adatvédelmi szabályozás tükrében kétségtelenül lényeges szempontot képvisel.

A Google az MI szabályozás gyakorlati átültetésével kapcsolatosan ugyancsak különböző szempontokat foglal össze, amelyek figyelembevétele a piaci szereplők, valamint az MI alapú megoldások elterjedése számára hasznos lehet, ideértve például nyilvánosságra hozatali, illetve transzparenciával kapcsolatos követelményeket, illetve a kockázatértékeléssel kapcsolatos követelmények egyértelmű megfogalmazását.

A Meta csoport – saját nyilatkozata szerint – 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 előre lépéseket tett például az adatvédelmi oktatás, az adatvédelmi kockázatértékelés- és kezelés, valamint az adattovábbítások és azok átláthatósága területén is.[116]

A fentiek mellett a Facebook meghatározta a felelős MI fejlesztés és alkalmazás öt oszlopát, amelyeket a Facebook esetén a Meta figyelembe vesz, ideértve

- adatvédelem és védelem,
- tisztesség és befogadás,
- megbízhatóság és biztonság,
- átláthatóság és irányítás,
- elszámoltathatóság és kormányzás.[117]

Mint az a fentiekből is látszik tehát, mind a Meta csoport, mind azon belül a Facebook a többi technológiai vállalathoz hasonlóan, a nyilvános kommunikációiban rögzítettek szerint jelentős

[116] 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 [2023.07.09.]
[117] Meta AI, Facebook’s five pillars of Responsible AI, 2021.06.22, https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/ [2023.07.09.]

figyelmet igyekszik fordítani az adatvédelmi megfelelésre, valamint az MI etikai alapelvek mentén történő fejlesztésére és alkalmazására.

A fentieken túl a Microsoft technológiai vállalat is meghatározta a felelős MI alapelveit (angolul: „*responsible AI principles*"), ideértve az alábbiakat:

- tisztesség,
- megbízhatóság és biztonság,
- adatvédelem és védelem,
- befogadás – ideértve mindenki bevonását és támogatását,
- átláthatóság,
- elszámoltathatóság.[118]

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 általános alkotmányos, illetve emberi jogi követelményeket jelenítenek meg, amelyek számos esetben az irányadó regionális vagy nemzeti adatvédelmi szabályozásban is figyelmet élveznek (például: tisztesség, átláthatóság, elszámoltathatóság).[119]

Az IBM a megbízható MI kapcsán a fentiekhez részben hasonló alapelveket határozott meg, ideértve

- az MI azon célját, hogy felerősítse az emberi intelligenciát, ne pedig leváltsa azt,
- az adatok és meglátások alkotóhoz tartozását,
- a technológia átláthatóságát és megmagyarázhatóságát.[120]

A fentiek szerint tehát az IBM külön hangsúlyozza az MI azon célját, hogy felerősítse és támogassa az emberi intelligenciát, ne pedig annak pótlékaként vagy – ad absurdum – következő lépcsőfokaként tekintsünk rá. Emellett az IBM fenti kommunikációjában ugyancsak hangsúlyozza a különböző, MI-hez kapcsolódó adatok és meglátások alkotóhoz való tartozását

[118] Microsoft, Putting principles into Practice at Microsoft, https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimaryr5 [2023.07.09.]
[119] Lásd például a GDPR 5. cikke szerinti alapelveket.
[120] IBM, From principles to actions: building a holistic approach to AI governance, https://www.ibm.com/blog/from-principles-to-actions-building-a-holistic-approach-to-ai-governance/ [2023.07.08.]

és az alkotó jogait (bizonyos értelemben hasonlóan például a szellemi alkotások területén a mű és az alkotó közötti viszonyhoz), továbbá a technológia átláthatóságának és megmagyarázhatóságának, nyomon követhetőségének fontosságát.

Ahogy az a fentiekből is látszik tehát, mind az államok, mind a nemzetközi és egyéb szervezetek, valamint a technológiai szektor szereplői számos szempontból hasonlóan határozták meg az MI fejlesztésével, valamint használatával kapcsolatos alapelveket. Habár az egyes szervezetek, szereplők által meghatározott alapelvek listáján és a kapcsolódó kommunikációkon „áthallatszanak" az adott szereplők érdekei, valamint az általuk felvázolt esetleges problémakörök is, ezek számos esetben hasonló, etikai és jogi szempontból is kiemelkedő, alapvető követelményeket határoznak meg. Így jellemzően az alábbi alapelvek jelennek meg közös pontként az egyes államok, nemzetközi szervezetek, valamint a technológiai iparág szereplői anyagjaiban és kommunikációiban:

- tisztesség,
- az érintettek érdekeinek figyelembevétele,
- átláthatóság,
- adatvédelem,
- megbízható és biztonságos alkalmazás,
- kockázatértékelés.

Kiemelendő, hogy bár a fenti alapelvek 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 és alkalmazás esetén 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 megfogalmazhatók (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 segíti.[121]

iv. Hogyan szabályozzuk az MI-t?

Az MI szabályozás alapelveinek, a szabályozás körének és jogosultjainak, valamint keretrendszerének meghatározásán túl jelentős kérdés marad a szabályozás megfelelő módjának és mértékének megválasztása, valamint ennek kapcsán az adott terület felügyelete.
A megfelelő szabályozás kialakítása kapcsán álláspontunk szerint a kockázatalapú megközelítés tekintendő irányadónak. Ezen meglátásokat az MI Rendelet Tervezet is tükrözi, tekintettel arra, hogy az adott MI-rendszer, illetve alkalmazásának kockázatait figyelembe véve határoz meg tilalmakat, illetve támaszt különböző követelményeket. Ennek során különös jelentősége van az adott megoldás vagy rendszer fejlettségének és önállóságának, valamint az alkalmazás céljának és módjának, az érintettek körének, valamint az adott rendszer érintettekre gyakorolt hatásainak.

A fentiek körében megemlítendő, hogy egy általánosnak tekinthető MI megoldás általában véve jelentősebb hatással, illetve kockázatokkal bírhat az azt használó vagy az által érintett személyekre, tekintettel arra, hogy az emberi felülvizsgált ez esetben korlátozottabb, az adott rendszer pedig jellemzően többféle célból és módon is használható. Ugyanakkor megemlítendő, hogy egy bizonyos szempontból „önállónak" tekinthető MI-rendszer nem feltétlenül jelent jelentősebb veszélyt a társadalomra nézve, amennyiben az adott rendszer kialakításának, alkalmazásának egyéb körülményei nem teszik veszélyessé, ahogy önmagában az a tény, hogy egy ember kimondottan magas intelligenciával rendelkezik sem garancia arra, hogy kimondottan sikeres lesz vagy kiemelt társadalmi befolyással fog bírni. Napjainkban még nem érthetjük tisztán, egy emberi intelligenciához elméletileg hasonló „általános" MI hogyan is gondolna a világra, sajátmagára és az emberre, így az általános vagy magasabb fejlettségi szintű MI megoldásokkal szemben az egyetlen veszély a bizonytalanság marad, amelyre bizonyos

[121] Necz Dániel, A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. https://bm-tt.hu/wp-content/uploads/2022/02/2020_1.pdf. 135-165. 142.

szempontból orvosság lehet a megfelelően rugalmas szabályozás, amely arányos mértékű emberi felügyeletet követel meg a technológiai fejlődés túlzott visszaszorítása nélkül.

Az erős vagy általánosnak tekinthető MI esetén különböző szabályozási megközelítések képzelhetők el arra tekintettel, hogy az adott megoldás vagy az érintett terület, illetve az alkalmazás által érintett személyek jogainak vagy érdekeinek védelme milyen szintű szabályozói beavatkozást kíván. Így például – az európai MI szabályozás kockázatalapú megközelítését alkalmazva – a legveszélyesebb és leginkább káros rendszerek esetén arányos megközelítés lehet akár a teljes tilalom is, míg a bizonyos esetekben hasznos, azonban magas kockázattal bíró rendszerek esetén ezen kockázatok csökkentésére szolgáló intézkedések előírása tekinthető a legoptimálisabb szabályozói megközelítésnek. A fentiek kapcsán megjegyezzük azonban, hogy az egyes alkalmazások monopolizálását jellemzően nem tekintjük megfelelő szabályozói megközelítésnek, mivel ez jelentős versenykorlátozó hatással bírhat, és az MI-vel kapcsolatos fejlesztéseket is aránytalan mértékben korlátozhatja.

A fentieken túl kétségtelennek tekintendő azonban, hogy akár egy kevésbé fejlett MI alapú megoldás is adott esetben jelentős kockázattal bírhat az érintettekre, ideértve különösen a sérülékenyebb csoportok tagjait, mint például a gyermekeket, az időseket vagy a betegeket. Erre tekintettel is fontosnak tekinthető a sérülékeny csoportba tartozó érintettek érdekeit, valamint jogait és szabadságait, valamint a szektorspecifikus szempontokat figyelembe vevő szabályozás kialakítása (például: az egészségügyi területen történő MI alkalmazásra vonatkozó speciális szabályozás).

Az erős MI-vel szemben a gyenge MI azonban jellemzően enyhébb szabályozást igényel, hiszen ezen rendszerek használata általában kevésbé jár veszélyekkel az érintettekre, így elsősorban az adott rendszer egyes sajátosságai által indokolt követelmények előírása, illetve a szükséges mértékű átláthatóság megkövetelése tekinthető arányosnak. Bizonyos területeken kiemelten fontos lehet továbbá akár egyszerű MI-rendszerek esetén is az emberi felülvizsgálat megkövetelése. Így például ügyvédi irodák, jogi szolgáltatást nyújtó szervezetek és személyek által biztosított chatbot alkalmazások esetén észszerű előírás lehet a jogi tanácsadás, illetve jogi szolgáltatások kapcsán ügyvédi vagy más szakértői felülvizsgálat megkövetelése, a megfelelő felügyelet nélküli, MI általi jogi tanácsadás ugyanis adott esetben jelentős károkat okozhat az érintetteknek.

Természetesen a fenti logika alapján hasonló követelmények támaszthatók más szabályozott szakmák gyakorlói által alkalmazott gyenge MI megoldások kapcsán is, amennyiben azokat szabályozott tevékenység keretén belül használják fel (ideértve például egészségügyi szolgáltatás vagy pénzügyi szolgáltatás nyújtását, kapcsolódó tanácsadást). Kevésbé tekinthető azonban kockázatosnak általános, összefoglaló tájékoztatás nyújtása (például: eleve meghatározott menüpontok szerint), illetve az érintett szakértővel való kapcsolattartást segítő egyéb megoldások biztosítása (például: időpontfoglalás, az adott probléma vagy megkeresés tárgyának, illetve az illetékes szakértőnek az azonosítása a chatbot segítségével).

Mint az a fentiekből is látszik, a gyenge MI esetén az egyes szakmai szervezetek ön-, illetve társszabályozási szerepköre különös jelentőséggel bírhat, és segíthet azon esetek könnyebb azonosításában, amikor jelentősebb követelmények támasztására, illetve garanciák biztosítására van szükség az érintettek védelme, valamint a szakmai szabályok betartásának biztosítása érdekében.

Akár gyenge, akár erős MI-ről beszélünk azonban, a megfelelő szabályozásnak ajánlott kockázatalapú megközelítést alkalmaznia, amely az adott MI megoldás sajátosságait, az alkalmazás körülményeit és az érintett szolgáltatások, tevékenységek körét, valamint az azok által érintettek érdekeit is figyelembe veszi. Maga az európai MI szabályozás sarokkövét képező MI Rendelet Tervezet is kockázatlapú megközelítésből indul ki, ugyanis csak ennek révén biztosítható észszerűen, hogy a különböző kockázattal bíró MI-rendszerek alkalmazása esetén ezek súlyához igazodó, megfelelő szabályok kerüljenek alkalmazásra.[122]

A fentiek mellett érdemes azon is elgondolkoznunk azonban, hogy az emberi kontroll megőrzése minden esetben szükséges-e az MI megbízható alkalmazásához. Számos szabályozási megközelítésből ugyanis az tűnik ki, hogy az emberi kontroll a megbízható MI egyik alapvető garanciája,[123] azonban számos MI alapú alkalmazás épp az emberi eljárást vagy felügyeletet hivatott csökkenteni, illetve kiváltani. Az önvezető autók esetén az önvezetés egy magasabb fokán ugyanis az MI elvileg képes lesz arra, hogy akár egy gyermeket vagy egy látássérült embert is a kívánt célállomásra szállítson, mégpedig biztonságosabban, mintha mindezt egy emberi sofőr tenné. Értelemszerűen ezen esetekben nem várható el, hogy egy vezetésre nem jogosult vagy képes személy gyakoroljon felügyeletet a technológia felett, a

[122] MI Rendelet Tervezet (14) preambulum-bekezdés
[123] Lásd különösen: MI Rendelet Tervezet 14. cikk, GDPR 22 cikk (3) bek.

távoli segítségnyújtás (például: ügyfélszolgálaton vagy központon keresztül) pedig nem feltétlenül reagálhat elég gyorsan a technológia alkalmazásával járó valamennyi körülményre (például: a közlekedés dinamikájából, forgalmi helyzetekből származó körülmények, események). Ilyen esetekben tehát az emberi felügyelet vagy beleszólás kerülendő, vagy csak kivételesen foghat helyt (például: egyes gépjárművekhez tartozó rendszerek már most képesek érzékelni a vezető fáradtságát és szükség esetén jelezni azt vagy átvenni az irányítást).[124] Mindez természetesen nem jelenti azt, hogy az emberi felügyelet ne lenne kiemelt fontosságú az MI szabályozása és alkalmazása területén, hiszen az esetek többségében az emberi felügyelet, felülvizsgálat, valamint közrehatás valóban kiemelt jelentőséggel bír, és segítséget nyújt a technológia alkalmazásával kapcsolatos bizonytalanságok, kockázatok kiküszöböléséhez, valamint a technológia „emberarcú" jellegének megőrzéséhez. Vitatathatatlan tény azonban, hogy az MI alkalmazása egyes esetekben nagyobb fokú önállóságot vagy alacsonyabb mértékű, illetve módú emberi felülvizsgálatot követel meg, amelyet természetesen a szabályozásnak is megfelelő módon tükröznie kell.

Az MI megfelelő szabályozási megközelítésén túl további vitát képezhet az egyes MI alapú megoldások, valamint azok alkalmazásának felügyeletét ellátó szerv, illetve hatóság meghatározása, ezek illetékessége (például: általános vagy speciális MI hatóság). E körben az MI Rendelet Tervezet független felügyeleti hatóság létrehozását írja elő, valamint meghatározza az erre vonatkozó szabályokat.[125] Az illetékes MI hatóságon túl azonban számos esetben szakhatóság vagy más szakértő bevonására is szükség lehet, különösen olyan esetekben, ahol az MI alkalmazása olyan meghatározott terület vagy területek szaktudását igényli, amelyet szakhatóság, illetve külön ezen a területen eljáró szakértők képesek biztosítani. Ilyen lehet például környezetvédelmi szakhatóság bevonásának szükségessége egy olyan építési projekt kapcsán, amely során az érintett építési terület által érintett környezeti adatok elemzését MI alapú technológiával végzik.

A fentiek mellett adott esetben a generatív MI kapcsán is felmerülhet sajátos szabályozás, illetve hatósági gyakorlat kialakításának szükségessége. Az ilyen megoldások sajátossága, hogy a betáplált információk, illetve utasítás alapján magas szintű szöveges, képi vagy egyéb

[124] Eric A. Taub, Sleepy Behind the Wheel? Some Cars Can Tell, The New York Times, 2017.03.16, https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html#:~:text=Through%20its%20Driver%20Availability%20Detection,drowsiness%20detection%20systems%20exist%20today. [2023.09.10.]
[125] MI Rendelet Tervezet VII. fejezet

tartalmakat hoznak létre.[126] Ezen megoldások számos esetben támogatják a szabadidő kreatív eltöltését, azonban jelentős üzleti lehetőségekkel is kecsegtetnek (ideértve például: generatív MI megoldás által létrehozott reklámanyagok, képek, zene felhasználása). A sajátos szabályos a fentiekre tekintettel különösen az adott alkotás által létrehozott művek vagy ahhoz kapcsolódó tevékenység, szolgáltatások kapcsán foghat helyt. Így e körben például jelentős szempontot képezhet a szellemi alkotások jogával kapcsolatos szabályozás, az esetleges szellemi tulajdonjog kapcsán illetékes hatóságok, tanácsadó vagy egyéb hasonló testületek eljárása, és az általuk kialakított gyakorlat. Emellett az egyes tartalmak, és az azok felhasználása által érintett további tevékenységek vagy szolgáltatások kapcsán felmerülhet például a médiahatóság illetékessége (ideértve például az MI által alkotott reklámtartalmakat), de akár a pénzügyi felügyeletet ellátó hatóság (például: chatbot alkalmazása banki szolgáltatások területén) vagy más hatóságok illetékessége is. Természetesen továbbá a generatív MI megoldások esetén is jelentősnek tekinthetők az adatvédelmi szempontok, illetve a felhasznált személyes adatok átlátható kezelése.[127]

Ugyancsak érdekes kihívást jelenthet a közeljövőben a szociális vagy egészségügyi robotok szabályozása. Ezek ugyanis jellemzően az egyéb MI alapú megoldásoknál közvetlenebb kapcsolatot alakítanak ki az emberekkel, ráadásul gyakran sérülékenyebb csoportok tekintetében kerülnek alkalmazásra (ideértve például: időseket, betegeket, gyermekeket). Ezen csoportok általános igényeinek figyelembevételén, illetve érdekeinek védelmén túl azonban kifejezetten szükséges lehet a társadalmi és kulturális sajátosságok figyelembevétele, ahhoz hasonlóan, ahogy azok az emberek közti kapcsolatokban is jelentőséggel bírnak (például: vallási, társadalmi előírások, a lehetséges körben nagyobb fokú figyelembevétele).

A fentieken túl azonban természetesen más területeken is felmerül sajátos szempontok alkalmazása, illetve sajátos szabályozási megoldások megkövetelése, ideértve például az MI toborzási és munkahelyi célú alkalmazását, amely kapcsán az Egyesült Államokban több állam is sajátos szabályozást vezetett be a munkavállalók védelme érdekében.[128] Mindez azért is fontos, mert a munkavállalók és az egyes álláshelyekre jelentkező személyek is hasonlóan kiszolgáltatott helyzetben vannak, a technológia kizárólag munkáltatói érdekeket figyelembe vevő alkalmazása pedig jelentős társadalmi igazságtalansághoz, a foglalkoztatással kapcsolatos

[126] What is generative AI? IBM, 2023.04.20, https://research.ibm.com/blog/what-is-generative-AI [2023.09.10.]
[127] Ennek kapcsán lásd az általunk a deepfake tartalmak kapcsán a vonatkozó fejezetben alább előadottakat.
[128] Lásd: a tanulmány amerikai állami MI szabályozást tárgyaló részét.

visszaélésekhez (például: bizonyos csoportokba tartozó személyekkel szembeni diszkrimináció) vezethet. Emellett azonban természetesen számos olyan terület képzelhető el, ahol hasonlóan körültekintő szabályozásra van szükség, különösen a hasonlóan kiszolgáltatott érintetti csoportok esetén.

A fentebb írtakkal összhangban kijelenthető, hogy az MI sok szempontból forradalmi változásokat hozott, és számos olyan előnnyel kecsegtet, amelyek alapjaiban könnyíthetik meg mindennapi életünket, továbbá újabb lendületet adhatnak az emberiség fejlődésének és a korábban leküzdhetetlennek tűnő akadályok leküzdésének, úttörő fejlesztések eléréséhez. Ugyanakkor leszögezendő, hogy az MI, valamint a kapcsolódó fejlesztések szabályozatlansága jelentős veszélyeket is rejthet magában, továbbá beláthatatlan kihívások elé is állíthatja az emberiséget (például: fejlett MI megoldások döntő pozícióba kerülése, vagy meghatározott helyzetekben az MI emberi felülvizsgálat nélküli döntése). Emellett a nem megfelelő szabályozás, valamint a technológia sok esetben szabályozatlan alkalmazása az egyes sérülékeny vagy kiszolgáltatott csoportokkal szembeni diszkriminációt is erősítheti. Az MI alkalmazásával kapcsolatos veszélyek megelőzése, valamint kockázatok kezelése kapcsán azonban teljes tilalom vagy átfogó korlátozások felállítása, bevezetése helyett javasolt lehet az MI fejlesztéseket alapjaiban támogató, és a veszélyekre és kockázatokra arányosan reflektáló szabályozási környezet kialakítását célul tűzni. Mindez segítséget nyújthat ugyanis abban, hogy az MI az emberiség segítője maradjon, amely megfelelően alkalmazható demokratikus társadalmi körülmények között.

3. Adatvédelem a digitalizáció korában

A digitalizáció az adatvédelmi szabályozást is jelentős, új kihívások elé állította, tekintettel arra, hogy az új technológiák, különösen az MI megfelelő alkalmazásához, fejlesztéséhez jellemzően jelentős mennyiségű információ, és sok esetben akár szenzitívnek mondható személyes adat felhasználása is szükséges, a transzparens, érintettek számára megfelelően átlátható adatkezelés pedig a digitális térben számos esetben csak nehezen biztosítható. Emellett természetesen számos egyéb nehézség is felmerül (ideértve például: az érintetti jogok online térben való gyakorlását vagy az érintettek online viselkedésének befolyásolása elleni intézkedések megtételét), amelyek leküzdéséhez a helyes szabályozói megközelítésen túl legalább annyira van szükség megfelelő társadalmi és technológiai válaszra is.

A jelen fejezetben a digitalizáció és az MI alkalmazásának európai és amerikai szabályozása kerül bemutatásra, ideértve az egyes szabályozási megközelítések sajátosságait és a főbb szabályozási kihívásokat. Kitekintés kerül továbbá az egyes további országok MI-vel és digitalizációval kapcsolatos szabályozására, valamint ezzel kapcsolatos fontosabb meglátásaira.

a. A digitalizáció és a mesterséges intelligencia szabályozása az Európai Unióban

i. A digitalizációval kapcsolatos szabályozás

A digitalizáció és az MI területén az európai szabályozás vezető szerepet tölt be, továbbá számos esetben mintaként szolgál az amerikai és egyéb szabályozások számára. Az EU 2015-ben hirdette meg európai digitális egységes piaci stratégiáját, amelynek célja, hogy az európai társadalmakat és gazdaságokat átsegítse a digitális korba, valamint, hogy a digitális gazdaság előnyeinek kihasználását biztosítsa. Az európai digitális egységes piaci stratégiája már a kezdeti években is jelentős sikereket ért el, ideértve az új, átfogó európai adatvédelmi szabályozás bevezetését, az online tartalmak határon átnyúló hordozhatóságának biztosítását, valamint a roaming díjak és az indokolatlan, területi alapú tartalomkorlátozások megszüntetését.[129]

A fentiek kapcsán – különösen a jelen mű témájára figyelemmel – kiemelt jelentőséggel bírt az Európai Általános Adatvédelmi Rendelet („**GDPR**”)[130] megalkotása, valamint bevezetése, amely a korábbi, 1995-ös európai adatvédelmi irányelvet[131] váltotta fel. Habár az irányelv a maga korában jelentős előrelépést jelentett az európai jogharmonizáció irányába, és az eltérő tagállami szabályozásból adódó hátrányok kiküszöbölése felé, a digitális gazdaság kialakulásával nyilvánvalóvá vált, hogy jelentősebb harmonizációs lépésekre lesz szükség az EU-n belül. Ezen igény és a kapcsolódó törekvések végül a GDPR megalkotásához vezettek, amely kapcsán az európai jogalkotó kétéves felkészülési időt biztosítva 2018. május 25-től

[129] Európai Tanács, Európai digitális egységes piac, Bevezetés, https://www.consilium.europa.eu/hu/policies/digital-single-market/ [2023.07.15.]
[130] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg), OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[131] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, OJ L 281, 23.11.1995, p. 31–50 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

rendelte alkalmazandónak a rendeletet az EU-n belül. Annak ellenére, hogy számos szervezet elsősorban adminisztratív teherként vagy kihívásként tekintett rá,[132] a GDPR az elmúlt években számos tekintetben bizonyított, az európai adatvédelmi hatóságokat tömörítő Európai Adatvédelmi Testület („**EDPB**") pedig számos kérdésben egységes jogértelmezést segítő iránymutatásokat fogalmazott meg, amelyek mind a hatóságok, mind az adatkezelők és adatfeldolgozók számára iránymutatásul szolgálnak. Emellett a GDPR által kialakított egységességi mechanizmus[133] keretében a határon átnyúló ügyekben is sor került a nemzeti adatvédelmi hatóságok, valamint az EDPB közötti együttműködésre, adott esetben a nemzeti felügyeleti hatóság döntésének felülvizsgálatára. Így például az Európai Adatvédelmi Testület több szempontból felülbírálta az illetékes ír adatvédelmi hatóság által a WhatsApp Ireland Limited-el szemben hozott határozatát, és ennek megfelelően a döntése módosítására szólította fel az illetékes ír hatóságot.[134] Kiemelendő továbbá, hogy 2023. nyarán benyújtásra került egy új, GDPR végrehajtásával kapcsolatos további eljárási szabályok megállapításáról szóló rendelet-tervezet, amely még könnyebbé tenné a panaszkezelést, valamint további eljárási szabályokat állapítana meg.[135]

A fentieken túl az elektronikus hírközlési adatvédelmi szabályozás területén is történtek előre lépések, még ha lassabb mértékben is, mint az európai digitális egységes piaci stratégia által életre hívott további szabályozási törekvések esetén. Így 2017-ben megjelent a 2002-es elektronikus adatvédelmi hírközlési irányelvet[136] felváltani hivatott új elektronikus hírközlési adatvédelmi rendelet javaslata,[137] amely jelentős harmonizációt tenne lehetővé az elektronikus hírközlési adatvédelem területén, valamint a megváltozott technológiai és gazdasági környezetre, illetve társadalmi viszonyokra tekintettel modernebb szabályozást kíván bevezetni.

---

[132] Domokos Márton, Gyakorlati tapasztalatok a GDPR-megfelelés során. In: Szabó Endre Győző (szerk.), Az Infotörvénytől a GDPR-ig, Ludovika Egyetem Kiadó, Budapest, 2021. 209-220. 209.
[133] GDPR 63. cikk
[134] Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf [2023.09.11.]
[135] Javaslat, az Európai Parlament és a Tanács Rendelete, az (EU) 2016/679 rendelet végrehajtásával kapcsolatos további eljárási szabályok megállapításáról, Brüsszel, 2023.7.4., COM(2023) 348 final, 2023/0202(COD)
[136] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), OJ L 201, 31.7.2002, p. 37–47 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)
[137] Javaslat, Az Európai Parlament és a Tanács Rendelete, az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), Brüsszel, 2017.1.10. COM(2017) 10 final, 2017/0003(COD)

A fentieken túl az EU-n belül alkalmazandó fogyasztóvédelmi szabályok is jelentős módon korszerűsítésre kerültek a 2019. végén megjelent, ún. Omnibus-irányelv[138] révén, amely a modern társadalmi és gazdasági viszonyoknak jobban megfelelő, digitális kereskedelemre vonatkozó szabályokat, valamint követelményeket vezet be, illetve állapít meg, amelyek hatékonyabban lehetnek képesek a fogyasztók jogainak védelmére, valamint jogérvényesítési lehetőségeik támogatására.

Emellett megemlítendő, hogy az európai digitális egységes piaci stratégia az adatgazdaság, valamint az adatokhoz való hatékonyabb hozzáférés területén is jelentős vívmányokat ért el. Így a 2019. júniusában megjelent, a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról szóló európai uniós irányelv további könnyítést tett lehetővé a közszféra által kezelt információkhoz való hozzáféréshez, valamint az információszabadság kiteljesedéséhez.[139] Emellett a 2022. februárjában megjelent adatmegosztási jogszabály tervezete[140] jelentős könnyítéseket vezetett be a magán- és a közszféra szereplői számára az adatok megosztása, valamint az azokhoz való könnyebb hozzáférés vonatkozásában, továbbá a 2022. májusában megjelent adatkormányzási rendelet[141] például alapvető szabályokat vezetett be a közszféra által használt egyes adatok újra-hasznosítására, valamint az adatok önkéntes megosztására (adataltruizmus) vonatkozóan.

A fentiekből adódóan tehát az információkhoz való könnyebb hozzáférés, valamint az információk megosztásának megkönnyítése az európai digitális szabályozás egyik sarokkövévé vált. Ezen szabályozás a digitális gazdaság, valamint egy átláthatóbb és igazságosabban működő társadalom számára is jelentős motorként szolgálhat, az MI jelentette technológiai

[138] Az Európai Parlament és a Tanács 2019/2161 irányelve (2019. november 27.) a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról, PE/83/2019/REV/1, OJ L 328, 18.12.2019, p. 7–28 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[139] Az Európai Parlament és a Tanács (EU) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
[140] Az Európai Parlament és a Tanács Rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály), Brüsszel 2022.2.23. COM(2022) 68 final, 2022/0047(COD)
[141] Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet), PE/85/2021/REV/1, OJ L 152, 3.6.2022, p. 1–44 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

előnyökkel ötvözve pedig még jelentősebb és dinamikusabb társadalmi és gazdasági fejlődéshez vezethet.

Szintén jelentős vívmánynak tekinthető a 2022. végén megjelent, digitális piacok főként versenyjogi szempontjait szabályozó, digitális piacokról szóló jogszabály (angolul: „*Digital Markets Act*", röviden: „*DMA*"),[142] valamint a digitális szolgáltatásokat, valamint az online platformok működését szabályozó, digitális szolgáltatásokról szóló rendelet[143] (angolul: „*Digital Services Act*", röviden: „*DSA*"). A DSA és a DMA jelentős szabályozást alakít ki az egyes online szolgáltatók kapcsán (ideértve különösen egyes jelentős platformszolgáltatókat), emellett az online térben további, a fogyasztókat védő, illetve a piaci versenyt biztosító szabályokat vezet be.

ii. A mesterséges intelligenciával kapcsolatos szabályozás

A fentiek mellett az elmúlt időszakban szintén jelentős jogfejlődésnek lehettünk tanúi az MI szabályozása területén. Így az Egyesült Államokhoz hasonlóan az Európai Unió is kiemelt figyelmet fordít az MI jelentette társadalmi és gazdasági előnyökre, valamint a technológia szabályozására. Az európai uniós szabályozó azonban elsődlegesen általános szabályozás bevezetésére törekszik, amelynek keretein belül az elmúlt években felmérte a technológia hatásait és az azzal járó előnyöket és kockázatokat, majd tisztázta azon alapelveket és alapvető követelményeket, amelyeket az MI szabályozás során érvényesíteni kíván.

A fentiekre tekintettel 2018 áprilisában jelent meg a Bizottság Közleménye a Mesterséges Intelligenciáról Európának,[144] 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 (angolul: „*High-Level Expert Group on*

[142] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) 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, OJ L 265, 12.10.2022, 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)
[143] 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), PE/30/2022/REV/1, OJ L 277, 27.10.2022, 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)
[144] 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN [2023.09.19.]

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.[145]

A fenti kezdeti lépéseket követően, 2018. decemberében jelent meg a Bizottság újabb közleménye, a mesterséges intelligenciáról szóló összehangolt tervről,[146] 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,[147] 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.[148]

---

[145] Commission appoints expert group on AI and launches the European AI Alliance, DIGIBYTE, Európai Bizottság, 2018. június 14, https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance [2023.04.11]

[146] 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, https://eur--lex-europa-eu.translate.goog/legal-content/EN/TXT/?uri=CELEX:52018DC0795&_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc [2023.09.19.]

[147] 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, https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019DC0168&from=FR [2023.04.11.]

[148] Lásd: Uo. 4.

A fenti dokumentumot követően 2020. februárjában jelent meg a „Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése”,[149] 2021. áprilisában pedig a Bizottság „A mesterséges intelligenciával kapcsolatos európai megközelítés előmozdítása”[150] 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 MI Rendelet Tervezet, amely a különböző MI-rendszereket kategóriákba sorolja, és ennek megfelelően állít fel velük, illetve tervezőikkel, alkalmazóikkal szemben különböző tilalmakat és követelményeket. A fenti tervezet áttekintését követően a Tanács 2022. decemberi olvasatában több szempontból felülvizsgálta („**MI Rendelet Tervezet Tanácsi Változata**”), ideértve az MI-rendszerek meghatározását, az egyes rendszerek kategorizálását és a kapcsolódó követelményeket.[151] Ezt követően 2023. június 14-én jelent meg az Európai Parlament jelentése az MI Rendelet Tervezet felülvizsgálatáról („**MI Rendelet Tervezet EP Változata**”),[152] amely a tervezet szövegét számos tekintetben tovább finomította, így a tervezetet az európai jogalkotó jelenleg a trilógusban vizsgálja. Hangsúlyozzuk, hogy a dolgozatban az alábbiak szerint elsődlegesen az MI Rendelet Tervezet Bizottság által javasolt eredeti szövegezését vettük alapul, azonban annak kapcsán, egyes különösen relevánsnak vélt rendelkezések vonatkozásában egyéb változatokra (ideértve különösen az MI Rendelet Tervezet EP Változatát) is kitértünk. Kiemeljük továbbá, hogy bár az ezen jogszabályban meghatározott követelmények csak egy része kapcsolódik a személyes adatok védelméhez, az MI Rendelet Tervezet számos egyéb, alábbiakban részletezett követelménye révén közvetetten is jelentős hatást gyakorol az MI általi adatkezelési műveletekre, tekintettel arra, hogy az MI-rendszerek (különösen ideértve a nagy kockázatú MI-rendszereket és a generatív MI-rendszereket) fejlesztőire, rendelkezésre bocsátóira, illetve használóira számos, ezen rendszerekkel kapcsolatos olyan átfogó követelményt ír elő, amelyek az adatkezelési műveletek megszervezésére és folytatására is kihatással bírnak.

---

[149] Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése, Brüsszel, 2020.2.19. COM(2020) 65 final, https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_hu?filename=commission-white-paper-artificial-intelligence-feb2020_hu.pdf [2023.04.16.]

[150] 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, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021DC0205 [2023.04.16.]

[151] 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/ [2023.08.06.]

[152] Európai Parlament, Jelentés - A9-0188/2023, 2023.05.22, COM(2021)0206, https://www.europarl.europa.eu/doceo/document/A-9-2023-0188_HU.html [2023.08.06.]

Az MI Rendelet Tervezet kapcsán leszögezendő továbbá, hogy a jogszabály az MI-rendszerek, nem pedig általánosságban az MI szabályozására hivatott. Ennek kapcsán az MI-rendszert akként határozza meg, mint „*olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek*”.[153] A fenti meghatározáson pontosított az MI Rendelet Tervezet EP Változata, amely az MI-rendszert akként határozza meg, mint olyan „*gépi-alapú rendszert, amelyet különböző szintű önállóság melletti működésre terveztek, és amely meghatározott vagy közvetett célkitűzések adott csoportja tekintetében olyan kimeneteket, például előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek fizikai vagy virtuális környezeteket befolyásolnak*”.[154]

Az MI Rendelet Tervezet szabályozásának címzettje elsősorban az MI-rendszer szolgáltatója. Az MI Rendelet Tervezet értelmében a szolgáltató „*olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely MI-rendszert fejleszt vagy fejleszttet, hogy azt saját neve vagy védjegye alatt – akár fizetés ellenében, akár ingyenesen – forgalomba hozza vagy üzembe helyezze*”.[155] Ennek tükrében az MI Rendelet Tervezet elsődlegesen az olyan személyekkel vagy szervezetekkel szemben állít fel követelményeket, amelyek a jogszabály által meghatározott MI-rendszereket fejlesztik vagy saját nevük alatt a piacon elhelyezik. Emellett azonban az MI Rendelet Tervezet az egyéb piaci szereplőkkel, illetve a felhasználókkal szemben is meghatároz bizonyos követelményeket, tekintettel arra, hogy ezek is végezhetnek ezen rendszerekkel kapcsolatban olyan tevékenységet, amelyek veszélyekkel, illetve kockázatokkal járhatnak az érintettek számára.

A fentebb említettek szerint az MI Rendelet Tervezet által biztosított szabályozás és az azzal kapcsolatos követelmények az MI-rendszerek kategóriába sorolására építenek. Segítségképpen az MI Rendelet Tervezet által meghatározott főbb kategóriákat az alábbi táblázatban foglaltuk össze néhány releváns példa megadása mellett. Ezen kategóriák azonban a jelen műben az alább írtak szerint kifejtésre is kerülnek, így még szélesebb képet adva az irányadó szabályokról.

[153] MI Rendelet Tervezet 3. cikk 1. pontja
[154] MI Rendelet Tervezet EP Változata 3. cikk 1. pontja
[155] MI Rendelet Tervezet 3. cikk 2. pontja

Az MI Rendelet Tervezet által meghatározott kockázati kategóriák:

Kategória	Példák
Tiltott MI-gyakorlatok/rendszerek	Személyek egy meghatározott csoportja viselkedésének torzítására alkalmazott egyes MI-rendszerek[156]
Nagy kockázatú MI-rendszerek	Egyes toborzás céljára használt MI-rendszerek[157]
Alacsony kockázatú MI-rendszerek	Generatív MI alkalmazások, ideértve például a chatbot alkalmazásokat
Elenyésző kockázatú vagy kockázatot nem jelentő MI-rendszerek	MI-alapú megoldást alkalmazó videójátékok

Kiemelendő azonban, hogy a fenti példák mellett is előfordulhatnak olyan megoldások vagy alkalmazási módok, amelyek egy-egy rendszer szigorúbb kategorizálását teszik szükségessé. Így például, ha egy MI-alapú videójáték olyan szubliminális vagy egyéb technikákat alkalmaz, amely az azt használó gyermekeket ön- vagy közveszélyes magatartásra sarkall, úgy adott esetben a tilalmazott kategóriába is tartozhat, annak ellenére, hogy általában az MI-alapú megoldást alkalmazó videójátékok (amelynek napjainkban a videójátékok jelentős része tekinthető) nem tekinthetők különösebben veszélyesnek az azt használó, ajánlott életkori kategóriába tartozó felhasználókra nézve. Mindez egyben azt is jelenti, hogy az MI Rendelet Tervezetben meghatározottakon túl az egyes rendszerek tervezőinek és szolgáltatóinak figyelembe kell venniük az irányadó egyéb jogszabályi rendelkezéseket (ideértve például: az egyes termékekre és rendszerekre vonatkozó, valamint az adatvédelmi, fogyasztóvédelmi és egyéb szektorális jogszabályi rendelkezéseket), valamint az érintettek érdekeit.

A fentiekkel összhangban tehát az MI Rendelet Tervezet kockázatalapú megközelítést alkalmaz, amely tükrében az MI egyes alkalmazásait elfogadhatatlan kockázatúnak, míg egyes más alkalmazásokat nagy kockázatúnak, vagy éppen alacsony vagy minimális kockázatúnak tekint.[158] Az elfogadhatatlan kockázattal bíró alkalmazások körében az MI Rendelet Tervezet II. címben szereplő jegyzéke meghatározza mindazon MI-rendszereket, amelyek használata az

[156] MI Rendelet Tervezet 5. cikk (1) b) pontja
[157] MI Rendelet Tervezet III. melléklet 4. a) pontja
[158] MI Rendelet Tervezet, Indokolás, 5.2.2.

európai uniós értékeknek ellentmond, így elfogadhatatlannak minősül az Európai Unión belül.[159] Így tiltottnak minősülnek az olyan MI-gyakorlatokat megvalósító MI-rendszerek, amelyek

- szubliminális technikákat alkalmaznak az adott személy magatartásának tudatán kívüli torzításával,
- az adott csoport sebezhetőségét használják ki annak érdekében, hogy az adott csoporthoz tartozó személyek magatartását torzítsák, és ennek révén testi vagy lelki károsodást okozzanak nekik,
- hatóságok által vagy nevében kerülnek alkalmazásra, és amelyet természetes személyek megbízhatóságának értékelésére vagy osztályozására használnak, amely az érintett személyekkel szembeni diszkriminációhoz vezet olyan szociális kontextusban, amely nem függ össze azzal a kontextussal, amelyben az adatokat eredetileg létrehozták vagy gyűjtötték, illetve amely indokolatlan vagy aránytalan az érintettek közösségi magatartásához, vagy annak súlyosságához képest,
- „valós idejű" távoli biometrikus azonosító rendszerek használata a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból.[160]

A fentiek kapcsán hangsúlyozandó, hogy „valós idejű" távoli biometrikus azonosító rendszerek használatára az MI Rendelet Tervezet lehetőséget biztosít, amennyiben arra a) bűncselekmények konkrét potenciális áldozatainak felkutatása (például: eltűnt gyermekek vagy adott esetben más eltűnt személyek felkutatása), b) természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás megelőzése, vagy c) súlyos bűncselekmények (amelyek legalább háromévi szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel sújtandók) elkövetőinek azonosítása, illetve felelősségre vonása céljából kerül sor.[161] Kiemelendő, hogy ezen rendszerek alkalmazásának lehetőségét az MI Rendelet Tervezet EP Változata már nem tartotta fenn, és teljes egészében tilalom alá helyezte az ilyen rendszereket.[162]

Érdekes kérdésnek tekinthető, hogy a fenti tiltott rendszerek, alkalmazások alól kivételes esetekben tehetők-e kivételek, és ha igen, ezek kapcsán az adott MI-rendszer kivételes

[159] Uo.
[160] MI Rendelet Tervezet 5. cikk (1) bek.
[161] MI Rendelet Tervezet 5. cikk (1) d) pontja
[162] MI Rendelet Tervezet EP Változata 5. cikk (1) d) pontja

alkalmazásáról mely személy vagy hatóság jogosult dönteni, illetve milyen feltételek figyelembevételével. Például egy bankrablás során dönthet-e úgy a rendőrség, hogy az elkövetővel vagy elkövetők csoportjával 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). Ezt ugyanis adott esetben indokolttá teheti a bankban és környékén tartózkodó, túszul ejtett személyzet és látogatók, valamint a rendőri személyzet biztonságának védelme, valamint az elkövető elfogásához és felelősségre vonásához fűződő társadalmi érdek. Kérdéses azonban, hogy egy-egy ilyen eseti kivétel jóváhagyása mennyire tenné indokolttá a technológia széleskörben történő alkalmazását, illetve mennyire teremtene precedenst akár más kisebb súlyú, vagy a technológia alkalmazását kevésbé indokolttá tevő esetekben.

A fenti tiltott gyakorlatok és különös kockázatot jelentő rendszerek meghatározásán túl az MI Rendelet Tervezet ugyancsak meghatározza az ún. nagy kockázatú MI-rendszereket, amelyek fejleszthetők, illetve szolgáltathatók, az ezek által jelentett kockázat azonban még mindig nagynak tekinthető, így az európai jogalkotó szükségesnek tartotta ennek kapcsán további követelmények előírását, amelyek ezen kockázatokat kiküszöbölik, illetve csökkentik.

A nagy kockázatú MI-rendszerek kapcsán az MI Rendelet Tervezet meghatározza azon területeket, illetve ennek kapcsán az olyan rendszereket és alkalmazási megoldásokat, amelyek az érintettekre, valamint a demokratikus társadalom működésére jelentős kockázatokkal járnak. Az MI Rendelet Tervezet meghatározása szerint e körbe tartoznak az alábbi területeken alkalmazott, illetve alábbiak szerinti MI-rendszerek:

- Természetes személyek biometrikus azonosítása és kategorizálása;
- Kritikus infrastruktúra irányítása és működtetése körében használt rendszerek, e körbe értve a közúti forgalom, valamint az alapvető közművek irányítása, működtetése keretében használt MI-rendszereket;
- Az oktatás és szakképzés során az intézményekhez való hozzáférés, felvétel, értékelés keretében használt MI-rendszerek (például: hallgatók értékelése, egyetemi felvételi követelményeknek való megfelelés meghatározása);
- A foglalkoztatás keretén belül alkalmazott MI-rendszerek, ideértve a toborzás és a kiválasztás, értékelés, feladatkiosztás, szerződéses kapcsolatok előmozdítása vagy

megszüntetése kapcsán hozott döntések meghozatala körében alkalmazott MI-rendszereket;

- Alapvető magánszolgáltatásokhoz, közszolgáltatásokhoz és előnyökhöz való hozzáférés keretén belül alkalmazott MI-rendszerek, ideértve a hatóságok által vagy nevükben állami segítségnyújtási ellátásokra és szolgáltatásokra vonatkozó jogosultság, ennek csökkentése, visszavonása, visszaigénylések kapcsán hozott döntések körében alkalmazott MI-rendszereket, továbbá természetes személyek hitelképességének, hitelpontszámának megállapítása körében alkalmazott, vészhelyzeti első reagálási szolgáltatások biztosítása körében alkalmazott MI-rendszereket;
- Bűnüldözés során alkalmazott MI-rendszereket;
- Migráció, menekültügy, illetve határellenőrzés területén alkalmazott MI-rendszereket;
- Igazságszolgáltatás és demokratikus folyamatok során történő olyan MI-rendszerek alkalmazása során, amelyek az igazságügyi hatóságokat a tények és alkalmazandó jog kutatása során, valamint annak az adott tényállásra való alkalmazása körében segítik.[163]

A fentiek körében hangsúlyozandó, hogy az MI-rendszerek bűnügyi területen történő alkalmazása körében az MI Rendelet Tervezet azon területeket, illetve alkalmazási módokat határozza meg, amelyek az érintettek jogai és érdekei, valamint a demokratikus társadalom érdekei és 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. Így e körbe tartozik a bűnüldöző hatóságok által MI-rendszerek

- alkalmazása egyedi kockázatértékelés szempontjából (például: annak felmérésére, hogy az érintett milyen kockázatot jelenthet bűncselekmények újbóli elkövetése szempontjából);
- poligráfként vagy hasonló eszközként, valamint érzelmi állapot észlelésére szolgáló alkalmazása;
- deepfake-ek felderítésére szolgáló alkalmazása;
- bűncselekményekkel kapcsolatos nyomozás, valamint büntetőeljárás során bizonyítékok megbízhatóságának értékelésére történő felhasználása;
- potenciális bűncselekmények előfordulásának vagy megismétlődésének előrejelzésére történő felhasználása természetes személyek vagy csoportok kapcsán ezek jellemzői, tulajdonságai, múltbeli bűnöző magatartásának értékelése alapján;

[163] MI Rendelet Tervezet III. sz. melléklete

- profilalkotás céljára való felhasználása bűncselekmények felderítése, nyomozás, illetve védeljárás lefolytatása során;
- bűncselekmények elemzésére szolgáló felhasználását összetett, és egymással össze nem függő nagy adathalmazokban való keresés révén, minták azonosítása és rejtett összefüggések feltárása érdekében.[164]

A fentiekkel összhangban az MI Rendelet Tervezet elsődlegesen az MI-rendszerek diszkriminációra alapot adó vagy vélhetőleg ahhoz vezető, illetve a magánszférába való aránytalan behatást eredményező vagy alkotmányos elvekkel össze nem egyeztethető alkalmazását igyekszik meggátolni, természetesen nem célja az MI bűnüldöző szervek általi felhasználásának teljes és általános tilalmazása, azonban e tekintetben jellemzően több korlátozást érvényesít, illetve erősebb garanciákat követel meg a szabályozás a társadalom és az egyének jogainak és szabadságainak védelme érdekében.

A migráció és a menekültügy területén az MI Rendelet Tervezet szintén meghatároz olyan megoldásokat, illetve alkalmazási módokat, amelyek az emberi jogok tekintetében kirívó sérelemmel járhatnak, ideértve – a bűnügyi alkalmazás körében előadottakhoz hasonló módon – a poligráfként vagy hasonló eszközként történő felhasználást, a kockázatértékelést, úti okmányok és támogató dokumentumok ellenőrzése, valamint a menedékjog iránti kérelmek, vízumkérelmek, illetve tartózkodási engedélyek, jogállásra vonatkozó kérelmek, kapcsolódó panaszok kivizsgálása érdekében történő felhasználást.[165] Mindez azért is jelentős, mivel az algoritmus általi hiba vagy téves mintakövetés ezen a területen könnyen diszkriminatív gyakorlat kialakításához (például: bizonyos országból, területről származók vízum-kérelmeinek visszautasítása), illetve történelmi igazságtalanságok bebetonozásához vezethet.[166]

A fentiek tükrében tehát elmondható, hogy a nagy kockázatú MI-rendszerek kapcsán az MI Rendelet Tervezet elsődlegesen olyan megoldásokra, valamint alkalmazási módokra fókuszált, amelyek kiemelt kockázatokkal járhatnak mind az érintettek jogaira és szabadságaira, mind a

[164] MI Rendelet Tervezet III. sz. melléklet, 6. pontja
[165] MI Rendelet Tervezet III. sz. melléklet, 7. pontja
[166] 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, T.M.C. Asser Press The Hague, 2022. 187-204. 200.

demokratikus intézményrendszerekre. Ezek tekintetében kiemelt figyelmet kaptak a különböző pontozásra és értékelésre szolgáló megoldások, amelyek széleskörű alkalmazása a nyugati demokratikus társadalmakban idegennek tekinthető, valamint a biometrikus azonosítással, különböző alapvető szolgáltatások nyújtásával és üzemeltetésével, illetve a bűnügyi hatóságok eljárása vagy az idegenrendészet területén történő eljárásokkal kapcsolatos alkalmazásra szolgáló MI-rendszerek. Természetesen ezen, az MI Rendelet Tervezet mellékletében felállított lista nem tekinthető örök időkre kőbe vésettnek, hiszen a technológia fejlődésével, valamint a társadalmi és gazdasági folyamatok változásával egyes alkalmazási módokkal járó kockázatok csökkenhetnek, míg adott esetben újabb magas kockázattal járó 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, terrorcselekmények 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 a technológia például meghatározott vezetői vagy olyan pozíciókra, jelentős felelősséggel járó munkakörökben történő kiválasztás során lehet hasznos, ahol a teljesítmény és az eredmények mérhetők (például: pilóták esetén repülési szimulációk során tanúsított pontosság). Álláspontunk szerint azonban ezen alkalmazások esetén is szükségesnek mutatkozik az emberi felülvizsgálat, valamint az MI általi diszkrimináció elkerülésével kapcsolatos fokozott figyelem, amely kapcsán így csökkenthetők a hibás vagy diszkriminatív döntésekből eredő kockázatok. Emellett álláspontunk szerint továbbá a teljeskörű vagy a társadalom nagyobb részét érintő pontozás önmagában is kiemelt társadalmi kockázatokkal járhat.

A nagy kockázatú MI-rendszerekre vonatkozó követelményeket az MI Rendelet Tervezet 2. fejezete tartalmazza. Ezen kötelezettségek közé tartoznak az alábbi követelmények:

- kockázatkezelési rendszer,[167]
- adatokkal és adatkormányzással kapcsolatos követelmények,[168]

[167] MI Rendelet Tervezet 9. cikk
[168] MI Rendelet Tervezet 10. cikk

- műszaki dokumentáció elkészítése és naprakészen tartása,[169]
- naplózás és nyilvántartás,[170]
- átláthatóság és a felhasználók tájékoztatása,[171]
- emberi felügyelet biztosítása,[172]
- pontosság, stabilitás és kiberbiztonság biztosítása.[173]

A fentiekre tekintettel a nagy kockázatú MI-rendszerek esetén szükséges kockázatkezelési rendszer létrehozása, bevezetése, dokumentálása és fenntartása.[174] Az MI Rendelet Tervezet értelmében a kockázatkezelési rendszer egy „*olyan megszakítás nélkül végzett iteratív folyamat, amely a nagy kockázatú MI-rendszer egész életciklusát végigkíséri, és amelyhez az adatok rendszeres és szisztematikus aktualizálására van szükség*”.[175] Ezen folyamat továbbá legalább a következő lépéseket tartalmazza:

- ismert és előrelátható kockázatok azonosítása, elemzése,
- a nagy kockázatú MI-rendszer rendeltetésszerű használata és az észszerűen előre látható rendellenes használat becslése, értékelése,
- megfelelő kockázatkezelési intézkedések elfogadása.[176]

Annak érdekében továbbá, hogy a kockázatkezeléshez szükséges legmegfelelőbb intézkedések azonosíthatók legyenek, a nagy kockázatú MI-rendszereket tesztelni szükséges;[177] az ezzel kapcsolatos tesztelési eljárásoknak az adott rendszer rendeltetésének teljesítésére egyben alkalmasnak is kell lenniük, továbbá a cél eléréséhez szükséges mértékre kell korlátozódniuk.[178]

Az MI Rendelet Tervezet az adatokkal való tanítást magukban foglaló technikákat használó nagy kockázatú MI Rendszerek kapcsán minőségi kritériumokat határoz meg, így ezen rendszereket ezen kritériumoknak megfelelő tanulóadat-, érvényesítésiadat- és tesztadatkészletek alapján szükséges fejleszteni.[179] Ezen adatkészletek relevánsak,

[169] MI Rendelet Tervezet 11. cikk
[170] MI Rendelet Tervezet 12. cikk
[171] MI Rendelet Tervezet 13. cikk
[172] MI Rendelet Tervezet 14. cikk
[173] MI Rendelet Tervezet 15. cikk
[174] MI Rendelet Tervezet 9. cikk (1) bek.
[175] MI Rendelet Tervezet 9. cikk (2) bek.
[176] Uo.
[177] MI Rendelet Tervezet 9. cikk (5) bek.
[178] MI Rendelet Tervezet 9. cikk (6) bek.
[179] MI Rendelet Tervezet 10. cikk (1) bek.

reprezentatívak, hibáktól mentesek és teljesek kell, hogy legyenek, továbbá olyan statisztikai tulajdonságokkal kell rendelkezniük, amely megfelel azon érintettek csoportjainak, amelyek vonatkozásában az adott rendszert használni kívánják,[180] továbbá a rendszer használata által indokolt egyéb releváns jellemzőket és elemeket is szükséges figyelembe venniük.[181]

A nagy kockázatú MI-rendszerek esetén ezen túl még a forgalomba hozatala, illetve üzembe helyezés előtt műszaki dokumentációt kell készíteni, valamint ezen dokumentációt naprakészen vezetve tartani.[182] Az MI Rendelet Tervezet EP Változata ezen pont kapcsán a kis- és középvállalkozások esetén elegendőnek tartja az MI Rendelet Tervezetben előírtaknak megfelelő helyett ezen céloknak megfelelő egyéb dokumentáció elkészítését és rendelkezésre állását az illetékes nemzeti hatóság elfogadása mellett,[183] így ennek értelmében az Európai Parlament a kis- és középvállalkozások esetén könnyítés biztosítását látja szükségesnek a dokumentációs terhek alól.

Emellett az MI Rendelet Tervezet értelmében a nagy kockázatú MI-rendszereket olyan képességekkel ellátva kell megtervezni, illetve fejleszteni, amely lehetővé teszi az események automatikus rögzítését (naplózását) a rendszer működése közben; ezen naplózási képességeknek továbbá meg kell felelniük az irányadó szabványoknak vagy egyéb egységes előírásoknak.[184] A fenti naplózásnak az MI-rendszer teljes életciklusát végig kell kísérnie,[185] hogy biztosítható legyen az MI-rendszer megfelelő fejlesztése, illetve biztosítása. Az MI Rendelet Tervezet EP Változata a fentieken túl előírja továbbá a nagy kockázatú MI-rendszerek olyan naplózási képességekkel való ellátását is, amelyek az energiafogyasztást és a környezeti hatásokat is mérik,[186] így biztosítva a fenntartható fejlesztést és felhasználást.

A nagy kockázatú MI-rendszerek kapcsán kiemelt jelentőséggel bír továbbá az átláthatóság biztosítása, és a felhasználók 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. Ennek keretében az ilyen MI-rendszereket olyan módon kell megtervezni és

[180] MI Rendelet Tervezet 10. cikk (3) bek.
[181] MI Rendelet Tervezet 10. cikk (4) bek.
[182] MI Rendelet Tervezet 11. cikk (1) bek.
[183] MI Rendelet Tervezet EP Változata 11. cikk (1) bek.
[184] MI Rendelet Tervezet 12. cikk (1) bek.
[185] MI Rendelet Tervezet 12. cikk (2) bek.
[186] MI Rendelet Tervezet EP Változata 11. cikk (2a) bek.

fejleszteni, hogy a felhasználók a rendszer kimenetét értelmezni legyenek képesek, illetve azt megfelelően használhassák.[187] Az ilyen rendszerekhez továbbá használati utasítást kell mellékelni, ”*amely tömör, teljes körű, pontos és egyértelmű, a felhasználók számára releváns, hozzáférhető és érthető információkat tartalmaz*”.[188]

A fentiek kapcsán kiemelendő azonban, hogy az MI Rendelet Tervezet EP Változata pontosított, illetve bizonyos szempontból enyhített a fenti tájékoztatási kötelezettségen, tekintettel arra, hogy megfelelő tájékoztatást követel meg, amely elsődlegesen a rendszer funkciójára vonatkozik, illetve a rendszer céljával összhangban valósul meg. Olyan lehetséges körű intézkedéseket szükséges továbbá tenni, amelyek lehetővé teszik a kimenetel felhasználó általi értelmezését, illetve azt, hogy általában véve hogyan működik a rendszer és milyen adatokat használ fel. Értelemszerűen továbbá a használati utasításnak is ezen tájékoztatási követelményekhez kell igazodnia, lehetőség szerint teljeskörű információt nyújtva, amely segítséget nyújt a rendszer működtetésében és üzemeltetésében, valamint a felhasználó tájékozott döntéshozatalát is támogatja.[189]

A nagy kockázatú MI-rendszerek kapcsán kiemelt jelentőséggel bír továbbá az emberi felügyelet biztosítása. Ennek kapcsán megfelelő ember-gép interfész eszközök révén biztosítani szükséges, hogy a rendszert használatának időtartama alatt természetes személyek hatékonyan felügyelhessék.[190] Ezt MI Rendelet Tervezet EP Változata kiegészíti azzal, hogy a felügyeletet az adott rendszer által biztosított kockázatokkal arányosan kell biztosítani, továbbá a felügyeletet ellátó személyeknek megfelelő tudással (MI írástudás) kell bírniuk a rendszerről ahhoz, hogy megfelelő támogatást nyújthassanak, illetve felügyeletet láthassanak el, illetve egy esetleges incidens bekövetkezése esetén ezt kivizsgálhassák.[191] Az emberi felügyeletet a rendszerbe beépített intézkedések, és/vagy egyéb, a felhasználó általi alkalmazásra megfelelő intézkedésekkel kell biztosítani.[192]

Mindemellett az MI Rendelet Tervezet kiemeli továbbá, hogy „*nagy kockázatú MI-rendszereket úgy kell megtervezni és fejleszteni, hogy rendeltetésük fényében megfelelő szintű pontosságot,*

[187] MI Rendelet Tervezet 13. cikk (1) bek.
[188] MI Rendelet Tervezet 13. cikk (2) bek.
[189] MI Rendelet Tervezet EP Változata 13. cikk (1)-(2) bekezdései
[190] MI Rendelet Tervezet 14. cikk (1) bek.
[191] MI Rendelet Tervezet EP Változata 14. cikk (1) bek.
[192] MI Rendelet Tervezet 14. cikk (3) bek.

stabilitást és kiberbiztonságot érjenek el", amely követelményeknek a rendszerek teljes életciklusa során érvényesülnie kell.[193] Az MI Rendelet Tervezet EP Változata ennek kapcsán kiemeli a beépített és alapértelmezett biztonság követelményét, és az ennek megfelelő intézkedések alkalmazását.[194]

A a nagy kockázatú MI-rendszerek alkalmazása esetén az MI Rendelet Tervezet a szolgáltatón túl a forgalmazókra[195], importőrökre[196], felhasználókra[197] és bármely más harmadik félre is az ennek kapcsán a szolgáltatóra irányadó kötelezettségek alkalmazását rendeli, amennyiben e személyek vagy szervezetek

- ilyen rendszert saját nevük vagy védjegyük alatt hoznak forgalomba vagy helyeznek üzembe;
- a már forgalomba hozott vagy üzembe helyezett rendszer rendeltetését módosítják; vagy
- jelentősen módosítják a nagy kockázatú MI-rendszert.[198]

A jogszabály kiemeli továbbá, hogy az utóbbi két pontban foglalt körülmények valamelyikének fennállása esetén a rendszert eredetileg forgalomba hozó vagy üzembe helyező szolgáltató a jogszabály szerinti szolgáltatónak már nem tekinthető, és így rá az ezzel kapcsolatos követelmények sem vonatkoznak.[199] Az MI Rendelet Tervezet EP Változata a fenti rendelkezéseket némileg módosítja, és elsődlegesen a már forgalomba hozott rendszerek sajátként jelölése, illetve a jelentős módosítások esetén tekinti alkalmazandónak az eredetileg a szolgáltatóra irányadó felelősségi szabályokat, további követelményeket támaszt az egyes szereplők közti együttműködés kapcsán, valamint az egyes generatív rendszerekre is kiterjeszti a fenti rendelkezés alkalmazását.[200]

---

[193] MI Rendelet Tervezet 15. cikk (1) bek.
[194] MI Rendelet Tervezet EP Változata 15. cikk (1) bek.
[195] MI Rendelet Tervezet 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 anélkül, hogy befolyásolná a rendszer jellemzőit*".
[196] MI Rendelet Tervezet 3. cikk 6. pontja értelmében az importőr „*az Unióban letelepedett természetes vagy jogi személy, aki vagy amely az Unión kívül letelepedett természetes vagy jogi személy nevével vagy védjegyével ellátott MI-rendszert hoz forgalomba vagy helyez üzembe*".
[197] MI Rendelet Tervezet 3. cikk 4. pontja értelmében a felhasználó „*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 használja*".
[198] MI Rendelet Tervezet 28. cikk (1) bek.
[199] MI Rendelet Tervezet 28. cikk (2) bek.
[200] MI Rendelet Tervezet EP Változata 28. cikk

Az egyes MI-rendszerek megfelelő értékelése, tanúsítása, valamint az értékelési és tanúsítási folyamatok, eljárásrend egységesítése érdekében az MI Rendelet Tervezet megfelelőségértékeléssel, valamint tanúsítással kapcsolatos rendelkezéseket is meghatároz.[201] Emellett a jogszabály további, innovációt támogató intézkedéseket határoz meg, ideértve különösen szabályozói tesztkörnyezet kialakítását, szabályozási kezdeményezések, illetve bizonyos MI-rendszerek esetén.[202] A fentieken túl az MI Rendelet Tervezet létrehozza továbbá a magatartási kódexek keretrendszerét, amelynek keretében a nagy kockázatú MI-rendszerektől eltérő, egyéb MI-rendszerek vonatkozásában az MI-rendszerek szolgáltatói, illetve ezek képviselői olyan magatartási kódexeket dolgozhat ki, amelyek meghatározott szempontok szerinti kötelezettségvállalásokat tartalmaznak.[203] Ezáltal fontos társadalmi célok könnyebb elérése válhat lehetővé, valamint a technológia etikus használata is erősödhet.

Tekintettel arra, hogy az MI-rendszerek kapcsán a generatív MI jelentősége is egyre inkább nő, illetve a technológia jelentősen elterjedtnek tekinthető, így az MI Rendelet Tervezet, illetve az MI Rendelet Tervezet EP Változata külön szabályokat határoz meg a különböző autonómiával felruházott, szöveges, képi, hang-, illetve videótartalmak létrehozására szolgáló, generatív MI-rendszerekre[204] vonatkozóan, felismerve a technológia jelentőségét, valamint annak társadalmi és gazdasági hatásait. Az MI Rendelet Tervezet EP Változata így az interakcióra szánt, illetve generatív MI-rendszerek kapcsán átláthatósággal kapcsolatos követelményeket határoz meg[205] annak érdekében, hogy az azzal kapcsolatba kerülő felhasználók felismerjék a generikus MI alkalmazását, továbbá a technológia irányadó jogszabályi követelményekre, valamint a tudomány állására tekintettel lévő, biztonságos alkalmazását, az alapul fekvő modell olyan képzését, amely megfelelő védelmet biztosít a jogsértő használattal (például: szerzői jogot sértő tartalmak előállítása) szemben, megköveteli továbbá a rendszer fejlesztéséhez használt szerzői jog által védett adatok használatának összefoglalását, valamint ennek közzétételét.[206] Emellett a jogszabály a deepfake tartalmak kapcsán is különös tájékoztatási kötelezettséget ír elő.[207] A fentiekkel összhangban tehát a generatív MI megoldások kapcsán az európai jogalkotó meglátásai szerint is szükségesnek tűnik sajátos szabályok alkalmazása, amely elsődlegesen az ilyen rendszerek alkalmazásával kapcsolatos transzparenciát helyezi előtérbe, így a fenti

[201] MI Rendelet Tervezet 4-5. fejezetei
[202] MI Rendelet Tervezet V. cím
[203] MI Rendelet Tervezet IX. cím
[204] MI Rendelet Tervezet EP Változata 28b. cikk 4. pontja
[205] MI Rendelet Tervezet 52. cikk
[206] MI Rendelet Tervezet EP Változata 28b. cikk 4. pontja
[207] MI Rendelet Tervezet EP Változata 52. cikk 3. pontja

rendszerek használói tisztában lehetnek azzal, hogy generatív MI megoldással lépnek kapcsolatba és végeznek interakciókat. Megjegyezzük azonban, hogy egyes deepfake alkalmazások, valamint az ezek által létrehozott tartalmak például személyiségi jogsértés, zsarolás, kényszerítés politikai vagy más manipuláció céljára történő felhasználása a gyakorlatban különösen nagy veszélyeket jelenthet, így ilyen alkalmazási módok esetén megfontolandó lett volna tilalom elrendelése,[208] vagy ezen MI-rendszerek magas kockázatúvá minősítése, illetve ezek kapcsán szigorúbb szabályok előírása.

A fentiekre tekintettel a bírósági és hatósági jogértelmezés vélhetőleg különös jelentőséggel fog majd bírni a közeljövőben, az egyes MI-rendszerekkel kapcsolatos elvárások adatvédelmi szempontjainak, valamint az MI Rendelet Tervezet és az adatvédelmi jogszabályok követelményeinek és gyakorlatának együttes értelmezése kapcsán. Ennek kapcsán kiemelendő, hogy az MI Rendelet Tervezet eredeti szövegét adatvédelmi szempontból is több kritika érte, amely jellemzően a jogszabály-tervezet világosságával, valamint annak megközelítése és a GDPR követelményei közti különbségekkel, illetve az európai adatvédelmi gyakorlat elvárásainak figyelmen kívül hagyásával volt kapcsolatos. Ennek kapcsán adatvédelmi szempontból a leginkább relevánsnak az EDPB és az európai adatvédelmi biztos vonatkozó közös véleménye[209] tűnik, amely összefoglalja a jogszabály eredeti szövegével kapcsolatos főbb adatvédelmi aggályokat, illetve az annak orvoslására szolgáló főbb javaslatokat. E körben az 5/2021. Közös Vélemény kifejezetten felrója a jogszabály-tervezet azon megközelítését, amellyel egyes csoportok vagy a társadalom egészére jelentett számos kockázatot figyelmen kívül hagy (ideértve például a demokratikus társadalom működését veszélyeztető lehetséges hatásokat),[210] továbbá az MI Rendelet Tervezet kockázatalapú megközelítése kapcsán a jogszabály-tervezet releváns szövegezésének a GDPR-al való összhangját hiányolja.[211] A fentieken túl az 5/2021. Közös Vélemény többek között szintén hiányosságként rója fel, hogy a nagy kockázatú MI-rendszerek MI Rendelet Tervezet II. és III. mellékleteiben meghatározott listája több olyan megoldást sem tartalmaz, amelyek az érintettekre nézve jelentős kockázattal járhatnak (például: egészségügyi kutatások kapcsán alkalmazott rendszerek).[212]

[208] A kaliforniai deepfake szabályozás mintájára például a demokratikus társadalmak működése szempontjából megengedhető tartalmakat (például: paródia) elkülönítve a jogsértő, káros tartalmaktól.
[209] 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 („**5/2021. Közös Vélemény**”)
[210] 5/2021. Közös Vélemény 17. pontja
[211] 5/2021. Közös Vélemény 18. pontja
[212] 5/2021. Közös Vélemény 19. pontja

Az 5/2021. Közös Vélemény kiemeli továbbá több olyan rendszer tilalmának szükségességét, amelyet az MI Rendelet Tervezet magas kockázatúnak minősít, ideértve különösen az egyes rendőrségi megfigyeléssel kapcsolatos felhasználást. Ennek kapcsán a 5/2021. Közös Vélemény hangsúlyozza, miszerint „*MI rendőrségi és bűnüldözési célú használatához területspecifikus, pontos, előrelátható és arányos szabályokra van szükség, amelyeknek figyelembe kell venniük az érintett személyek érdekeit és a demokratikus társadalom működésére gyakorolt hatásokat*”.[213] Az 5/2021. Közös Vélemény ugyancsak szót emel, és általános tilalmat követel a közösségi pontozás kapcsán,[214] továbbá szorgalmazza, 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*”.[215] Emellett a dokumentum ugyancsak az MI általi érzelemfelismerés általános tilalma mellett foglal állást, amely tekintetében csak szűk körű kivételeket tart megengedhetőnek (ideértve az egészségügyi vagy a kutatási célú felhasználást).[216] Ennek kapcsán megemlítendő, hogy 2022-ben a 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 érintettek számára jellemzően átláthatatlan módon, az érdekmérlegelés nem megfelelő módon történő elvégzése alapján.[217]

Az 5/2021. Közös Vélemény kiemeli továbbá a magas kockázatú MI-rendszerek esetén az általában harmadik fél által végzendő előzetes megfelelősértékelés fontosságát,[218] hangsúlyozza továbbá, hogy a szabályozásnak a már használatban lévő MI-rendszerekre is ki kell terjednie.[219] Emellett a dokumentum további meglátásokat tesz az MI-rendszerek

[213] 5/2021. Közös Vélemény 27. pontja
[214] 5/2021. Közös Vélemény 29. pontja
[215] 5/2021. Közös Vélemény 32. pontja
[216] 5/2021. Közös Vélemény 35. pontja
[217] NAIH-85-3/2022.
[218] 5/2021. Közös Vélemény 37. pontja
[219] 5/2021. Közös Vélemény 38-41. pontja

fejlesztésének és alkalmazásának adatvédelmi szempontjai kapcsán, ideértve a tesztkörnyezetet[220] és az átláthatóságot.[221]

Az MI Rendelet Tervezeten túl az európai MI szabályozás azonban egyéb fejleményekkel is büszkélkedhet. Így az MI Rendelet Tervezetét 2022. szeptemberében egy újabb jelentős jogszabály-tervezet, a mesterséges intelligenciával kapcsolatos felelősségről szóló irányelv javaslat („**MI Felelősségi Irányelv Javaslat**")[222] követte, amely a különböző MI-alapú megoldásokkal kapcsolatban állapít meg felelősségi szabályokat. Így a jogszabály-tervezet értelmében, az MI szerződésen kívüli károkozásával kapcsolatos jogvitában a felperes (aki előzetesen e célból megkereste az alperest) kérelmére lehetőség nyílik arra, hogy kötelezzék az alperes MI szolgáltatót, „*hogy mutassa be az olyan konkrét nagy kockázatú MI-rendszerekre vonatkozóan rendelkezésére álló releváns bizonyítékokat, amelyek esetében felmerült a károkozás gyanúja, vagy a felperes kérelmére, elrendeljék az említett személyekkel szemben ezeknek a bizonyítékoknak a bemutatását*".[223] A fenti kérelem alátámasztása érdekében azonban a felperesnek a kártérítési igény megalapozottságának alátámasztásához szükséges tényeket és információkat kell előterjesztenie.[224] Amennyiben az alperes nem tesz eleget a fentiek szerinti bizonyítékok bemutatását vagy biztosítását elrendelő határozatnak, úgy az illetékes tagállami bíróság „*vélelmezi, hogy az alperes nem tett eleget valamely vonatkozó gondossági kötelezettségnek, aminek igazolására az adott kártérítési igény érvényesítése céljából e bizonyítékot szánták*."[225]

A fentieken túl az illetékes tagállami bíróág a kártérítési igényre vonatkozó felelősségi szabályok alkalmazása kapcsán vélelmezi „*az alperes felróható magatartása és az MI-rendszer által előállított kimenet, vagy a kimenet előállításának MI-rendszer általi elmulasztása közötti ok-okozati összefüggés fennállását*" az alábbi feltételek valamelyike esetén:

- az alperes bizonyította vagy a bíróság vélelmezte az alperes vagy olyan személy felróható magatartását, akinek magatartásáért az alperes felelős,

[220] 5/2021. Közös Vélemény 61-68. pontja
[221] 5/2021. Közös Vélemény 69-72. pontja
[222] Javaslat, az EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a szerződésen kívüli polgári jogi felelősségre vonatkozó szabályoknak a mesterséges intelligenciához való hozzáigazításáról (a mesterséges intelligenciával kapcsolatos felelősségről szóló irányelv), Brüsszel, 2022.9.28, COM(2022) 496 final, 2022/0303(COD), https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52022PC0496 [2023.04.16.]
[223] MI Felelősségi Irányelv Javaslat 3. cikk (1) bek.
[224] Uo.
[225] MI Felelősségi Irányelv Javaslat 3. cikk (5) bek.

- észszerűen valószínűsíthető az ügy körülményei alapján, hogy az alperes vagy a fenti személy felróható magatartása befolyásolta az MI-rendszer által előállított kimenetet vagy a kimenet előállításának ezen rendszer általi elmulasztását,
- a felperes bizonyította, hogy a kárt a fentiek szerinti kimenet vagy annak elmulasztása okozta.[226]

A fentieken túl a jogszabály-tervezet az MI tervezésével és fejlesztésével kapcsolatos olyan hibákat és körülményeket is meghatároz, amelyekre a felperes sikeres bizonyításának ki kell terjednie a felelősség megállapítása érdekében (például: az átláthatósággal vagy a kiberbiztonsággal kapcsolatos hiányosságok).[227]

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 digitális és MI szabályozás sok szempontból így is útmutatónak tűnik, és vélhetőleg mintaként szolgál majd az EU-n kívüli országok szabályozásai számára is a közeljövőben.

b. A digitalizáció és a mesterséges intelligencia szabályozása az Amerikai Egyesült Államokban

i. A digitalizációval kapcsolatos szabályozás

Az Egyesült Államok már több mint egy évszázada a technológia fellegvárának, valamint a világ egyik legerősebb gazdaságának tekinthető. Ennek tükrében nem meglepő, hogy a digitalizáció, valamint az MI-alapú megoldások fejlesztése, előnyeinek kihasználása területén is sok szempontból élenjárónak tekinthető, amelyhez az utóbbi időben ehhez méltó szabályozási törekvések is társulnak.

Az elmúlt időszakban különösen az adatvédelem területén vett lendületet az amerikai szabályozás, amelyre mind szövetségi, mind tagállami szinten a szektorspecifikus megközelítés jellemző, így általános adatvédelmi szabályokat jellemzően nem, inkább egy-egy sajátos

[226] MI Felelősségi Irányelv Javaslat 4. cikk (1) bek.
[227] MI Felelősségi Irányelv Javaslat 4. cikk (2) bek.

területre vagy adatkezelési műveletek egy típusára irányadó szabályokat találunk. Ez már a korábbi évtizedek adatvédelmi szabályozása tekintetében is irányadónak volt tekinthető, ahol jellemzően egy-egy jelentős szektor kapcsán került sor átfogó szabályozásra. Így például a Health Insurance Portability and Accountability Act („**HIPAA**")[228] elnevezésű szövetségi törvény egyes egészségügyi szolgáltatók általi adatkezelést szabályozza átfogó módon. Emellett külön szövetségi szabályozás irányadó egyes szektorális, például pénzügyi intézmények vagy a felsőoktatási intézmények általi, illetve a nemzetbiztonsági célú adatkezelésekre. Fontos azonban kiemelnünk, hogy az európai értelemben vett adatvédelem nem feleltethető meg teljesen az angol „privacy" kifejezésnek, amely a leginkább a magánszférát és annak védelmét takarja, így az amerikai adatvédelmi szabályozás is inkább a magánszféra védelmét és annak zavartalanságát helyezi előtérbe a személyes adatok tágan értelmezett védelme helyett.[229]

A fentieken túl az ezredfordulót követően jelentős hangsúlyt kapott a gyermekek adatainak védelmével kapcsolatos szabályozás, különösen az online térben, amely annak gyakran szabályozatlan, illetve jelentős anonimitásnak teret adó jellemzői miatt egyben kiemelt veszélyekkel is bírhat a gyermekek számára, egyben a gyermekek a felnőtteknél jóval nagyobb mértékben is manipulálhatók, és lehetnek célpontjai jogsértő vagy etikátlan reklámoknak. Ezen veszélyforrásokat felismerve hozta meg a Kongresszus a Children's Online Privacy Protection Act („**COPPA**") elnevezésű szövetségi jogszabályt,[230] amely alapvető követelményeket támaszt a gyermekek védelme érdekében az online térben, ideértve nagyobb fokú transzparenciát és elszámoltathatóságot a weboldalak üzemeltetői, illetve az online szolgáltatásokat nyújtók tekintetében. A gyermekek adatainak védelme kapcsán azonban több szempontból még inkább szigorúbbnak mondható követelmények bevezetését tervezi a Kids Online Safety Act („**KOSA**") elnevezésű jogszabály-tervezet,[231] amely számos online szolgáltatás kapcsán vezet be, többek között, tartalomkorlátozással, valamint életkorigazolással kapcsolatos követelményeket, illetve jelentős szülői felügyeleti jogokat biztosít a gyermekek és fiatalok internethasználata felett. A 2023-ban felülvizsgált tervezetet azonban több

[228] Health Insurance Portability and Accountability Act of 1996, https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [2023.08.06.]
[229] 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, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft, Budapest. 17-29. 20.
[230] Children's Online Privacy Protection Act, https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter91&edition=prelim [2023.08.06.]
[231] Kids Online Safety Act, https://www.congress.gov/bill/118th-congress/senate-bill/1409/text [2023.08.06.]

szempontból is jelentős kritika érte, főként civil szervezetek részéről, amelyek a tervezettel kapcsolatos számos bizonytalanságot, nehézkes értelmezhetőséget, valamint a gyermekek (például: LMBTQ+ közösségbe tartozó fiatalok) lehetséges körű veszélyeztetését is hangsúlyozták.[232]

A fentieken túl szintén jelentős hangsúlyt élveznek a pénzügyi intézmények és szolgáltatók (például: bankok, biztosítótársaságok) adatkezeléseivel kapcsolatos szabályok, ideértve különösen az ún. Gramm-Leach Bliley Act elnevezésű törvényt,[233] amely a pénzügyi szolgáltatók adatkezeléseivel, valamint az általuk alkalmazott adatbiztonsági intézkedésekkel kapcsolatos legfontosabb szabályokat rögzíti. Emellett a kibervédelmi szabályozás területén is jelentős lépések történtek szövetségi szinten. 2023. szeptemberében például benyújtásra került a Small Business Cyber Resilience Act, amely a kisvállalkozások kibervédelmi képességeit növelné, például kibervédelmi megoldások, információk, illetve képzés könnyebb elérhetőségével.[234]

A fentiek mellett a fogyasztókat védő szabályozás is többszinten érvényesül, így a szövetségi szint mellett az egyes államok is jellemzően különböző törvényeket hoznak a fogyasztók védelme érdekében számos termék vagy szolgáltatás, illetve iparág tekintetében. Az Amerikai Egyesült Államokban tagállami szinten különösen jelentősnek tekinthetők továbbá a fogyasztói adatok kezelésével kapcsolatos jogszabályok, amelyek egyben a tagállami adatvédelmi szabályozás egyik fő mozgatórugóját is képezik. A könnyebb áttekinthetőség végett az alábbi táblázatban foglaltuk össze a jelen dolgozat kéziratának lezárásáig elfogadott tagállami fogyasztói adatkezeléssel kapcsolatos törvényeket:

Állam[235]	**Törvény elnevezése**	**Hatálybalépés**

[232] Lauren Feiner, Lawmakers update Kids Online Safety Act to address potential harms, but fail to appease some activists, industry groups, CNBC, Tech, 2023.05.02., https://www.cnbc.com/2023/05/02/updated-kids-online-safety-act-aims-to-fix-unintended-consequences.html [2023.08.06.]
[233] Gramm Leach Bliley Act, https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm [2023.08.18.]
[234] Risch Leads Effort to Improve Small Businesses' Access to Cyber Security Resources, 2023.09.07, https://www.risch.senate.gov/public/index.cfm/pressreleases?ID=A39F60D7-657C-4B05-B707-D8FA31A05128 [2023.09.16.]
[235] A táblázat kidolgozásához az alábbi összefoglalás került alapulvételre: Anokhy Desai, US State Privacy Legislation Tracker, IAPP, utolsó felülvizsgálat: 2023.07.21., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [2023.07.21.]

Kalifornia	California Consumer Privacy Act (CCPA)[236] California Privacy Rights Act (CPRA)[237]	CCPA: 2020.01.01. CPRA: 2023.01.01.
Colorado	Colorado Privacy Act[238]	2023.07.01.
Connecticut	Connecticut Personal Data Privacy and Online Monitoring Act[239]	2023.07.01.
Indiana	Indiana Consumer Data Protection Act[240]	2026.01.01.
Iowa	Iowa Consumer Data Protection Act[241]	2025.01.01.
Montana	Montana Consumer Data Privacy Act[242]	2024.10.01.
Tennessee	Tennessee Information Protection Act[243]	2024.07.01.
Texas	Texas Data Privacy and Security Act[244]	2025.01.01.
Utah	Utah Consumer Privacy Act[245]	2023.12.31.
Virginia	Virginia Consumer Data Protection Act[246]	2023.01.01.

A fenti tagállami jogszabályok a GDPR-hoz hasonlóan jellemzően számos érintetti jogot biztosítanak, ideértve például a törléshez vagy a tiltakozáshoz való jogot, ez utóbbit például az automatizált döntéshozatal, illetve profilalkotás esetén.[247] Ezen tagállami jogok azonban nem tekinthetők egységesnek, egyes tagállamokban a fogyasztók jogai szélesebb vagy eltérő körben érvényesülhetnek. Így például Utah szabályozása nem biztosít a fogyasztók számára a

[236]California Consumer Privacy Act of 2020, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 [2023.05.06.]
[237] Uo.
[238] Colorado Privacy Act, https://leg.colorado.gov/bills/sb21-190 [2023.05.06.]
[239] Connecticut Personal Data Privacy and Online Monitoring Act, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022 [2023.05.06.]
[240] Indiana Consumer Data Protection Act, https://legiscan.com/IN/text/SB0005/id/2779850 [2023.05.07.]
[241] Iowa Consumer Data Protection Act, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262 [2023.05.07.]
[242] Montana Consumer Data Protection Act, https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231 [2023.06.05.]
[243] Tennessee Information Protection Act, https://legiscan.com/TN/text/HB1181/id/2672877 [2023.06.05.]
[244] Texas Data Privacy and Security Act, https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/07/hb00004f.pdf?la=en&rev=d2ece1e4cc0c4a708453ab079b7f00f4&hash=22A797B43BCDE288DA18FEB244DAF1A7 [2023.09.19.]
[245] Utah Consumer Privacy Act, https://le.utah.gov/~2022/bills/static/SB0227.html [2023.05.07.]
[246] Virginia Consumer Data Protection Act, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/ [2023.05.07.]
[247] Lásd például: CCPA 1798.185(16), Colorado Privacy Act 6-1-1303(20), Connecticut Data Privacy Act Sec. 4., Virginia Consumer Data Protection Act § 59.1-573. 5.

profilalkotás kapcsán tiltakozási jogot.[248] Az érintetti jogokon túl azonban számos egyéb követelmény is eltérő lehet (például: azon szervezetek köre, akikre a szabályozás kiterjed, a szabályozás által érintett személyes adatok, szankciók, eljárási szabályok, stb.). A fentiek körében kiemelkedőnek tekinthető Kalifornia állam szabályozása, amely európai mintára saját adatvédelmi hatóságot hozott létre („*California Privacy Protection Agency*").[249] Az új elfogadásra kerülő, Delete Act nevű törvény értelmében ezen hatóság felügyeli majd azt a 2026. január 1-től létrejövő rendszert, amelyben az érintettek a Kalifornia államban személyes adatok gyűjtését és eladását végző adatbrókerektől adataik törlését kérhetik.[250] Emellett Kalifornia 2022-ben szintén egy új törvényt fogadott el, California Age-Appropriate Design Code Act (röviden: „**CAADCA**") néven, amely olyan CCPA által szabályozott szolgáltatókra terjed ki, amelyek gyermekek által feltehetőleg használt online szolgáltatásokat, megoldásokat fejlesztenek, illetve nyújtanak.[251] A CAADCA – részben az európai adatvédelmi szabályozás mintájára – számos követelményt támaszt a fenti szolgáltatásokat, illetve megoldásokat kínálókkal szemben, ideértve például adatvédelmi hatásvizsgálat elvégzését, valamint nagyobb fokú átláthatóság biztosítását, ideértve az érintett gyermekek által érthető nyelven megfogalmazott tájékoztatás közzétételét. A jogszabály 2024. július 1-i hatályba lépése előtt azonban a NetChoice elnevezésű, online vállalkozásokat tömörítő szervezet pert indított a jogszabály alkotmányellenességére hivatkozva, tekintettel arra, hogy az álláspontjuk szerint sérti a szólásszabadságot (Első Alkotmánykiegészítés), cenzori szerepbe kényszerítve a szolgáltatókat, valamint olyan kormeghatározást előírva, amely adott esetben a szükségesnél több adat gyűjtésével járhat, így sértve az érintettek adatvédelmi jogait.[252]

ii. A mesterséges intelligenciával kapcsolatos szabályozás

Az utóbbi években az adatvédelem és a digitalizáció egyéb területei mellett jelentős lendületet kapott az amerikai MI szabályozás, amelynek tekintetében fordulópontot jelentett a Donald

[248] Utah Consumer Privacy Act § 13-61-201(4)
[249] CPRA 1798.185. (16)
[250] Senate Bill no. 362, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362 [2023.09.16.]
[251]The California Age-Appropriate Design Code Act, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false [2023.09.17.]
[252]Mengting Xu, Lawsuit Challenges Constitutionality of California Age-Appropriate Design Code, California Lawyers Association, https://calawyers.org/privacy-law/lawsuit-challenges-constitutionality-of-california-age-appropriate-design-code/ [2023.09.17.]

Trump elnök által aláírt, 2019. februárjában megjelent 13859. sz. elnöki rendelet, [253] 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 rendelkezését, célkitűzését:

- 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 a fentebb már említett Blueprint megjelenése is, amely lefekteti az amerikai MI szabályozás alapelveit, egyben alapokat és szabályozási keretrendszert is biztosít a közeljövő MI szabályozása számára az Amerikai Egyesült Államokban.

Ugyancsak jelentős fejleményt jelent az Algorithmic Accountability Act of 2022[254] elnevezésű törvény-tervezet („**Algorithmic Accountability Act**"), 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 kizárólag jelentős árbevétellel rendelkező, illetve jelentős számú érintettre hatással levő automatizált döntéshozatalt, illetve hasonló eljárásokat alkalmazó szolgáltatókra vonatkozik.[255] A törvény 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),[256] figyelembe véve, hogy ezen területeken a diszkrimináció kockázata jellemzően magasnak mondható.

[253] Executive Order 13859 of February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence [2023.08.07.]
[254] Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/6580/text [2023.08.07.]
[255] Algorithmic Accountability Act sec. 2(7)
[256] Algorithmic Accountability Act sec. 2(8)

A törvény egyben meghatározza a fenti megoldások, eljárások alkalmazóival szembeni követelményeket, valamint előírja hatásvizsgálat elvégzését és dokumentálását, továbbá az ennek során figyelembe veendő, illetve értékelendő szempontokat és körülményeket is.[257] E körben kiemelt jelentőséggel bír az érintetti jogok figyelembevétele, amelynek kapcsán az adott, automatizált megoldás, illetve eljárást alkalmazó szervezetnek tájékoztatnia kell az érintettet ezen megoldás, illetve eljárás alkalmazásáról, valamint biztosítania kell számára az ezzel szembeni tiltakozáshoz való jogot is.[258] 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.[259]

Az elmúlt időszakban az automatizált döntéshozatal 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-tervezet,[260] amely szintén az automatizált döntéshozatali eszközökkel kapcsolatban ír elő követelményeket. A fentieken túl Kalifornia állam a félrevezető, ún. deepfake tartalmakkal szemben is több szempontból példamutatónak tekinthető szabályozást vezetett be. Az AB 730. sz. törvény[261] a deepfake tartalmak választási manipuláció (például: egy jelöltet negatív színben feltüntető hamis felvételek nyilvánosságra hozatala), valamint félrevezető és rosszindulatú szexuális tartalmú felvételek (például: zsarolás vagy lejáratás céljából készített hamis pornófelvételek) kapcsán

[257] Algorithmic Accountability Act sec. 3-4
[258] Algorithmic Accountability Act sec. 4(8)(A)
[259] Algorithmic Accountability Act sec. 4(9)
[260] Assembly Bill No. 331, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=202320240AB331&version=20230AB33195AMD [2023.08.07.]
[261] AB 730, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201920200AB730&version=20190AB73093CHP [2023.08.08.]

történő alkalmazásával szemben lép fel, illetve helyez kilátásba szankciókat (ideértve: szabadságvesztés büntetést is). Hasonló törvény-tervezet került benyújtásra nemrég Pennsylvania államban is, amely szintén szankcionálni kívánja az MI által létrehozott, mások érdekeit sértő, manipulált szexuális tartalmakat.[262]

A fentieken túl több állam – ideértve például az automatizált munkavállalói döntéshozatal alkalmazása kapcsán New York államot,[263] az MI munkahelyi célú alkalmazásának átláthatósága kapcsán Massachusetts államot,[264] valamint az MI videóinterjúk során történő alkalmazása kapcsán Illinois államot[265] – a munkahelyi adatkezelések kapcsán is bevezetett automatizált döntéshozatallal kapcsolatos szabályokat, tekintettel arra, hogy ezen területen a munkaviszonyban gyengébb félnek tekinthető munkavállalók védelme erősebb szabályozást követelhet 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.[266] Ezen szabályok számos esetben tartalmaznak adatvédelmi szempontból jelentős rendelkezéseket, például: a technológia alkalmazásával és az MI általi adatkezelés átláthatóságával kapcsolatos követelményeket, 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 körben védeni, valamint a technológia etikus felhasználásának követelményét erősíteni.

c. A digitalizáció és a mesterséges intelligencia szabályozása az európai és amerikai szabályozáson túl

[262] H1063. sz. törvény-tervezet, https://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2023&sind=0&body=H&type=B&bn=1063 [2023.09.19.]
[263] 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 [2023.08.14.]
[264] An Act Preventing a Dystopian Work Environment (H.1873) törvény-tervezet, https://malegislature.gov/Bills/193/H1873 [2023.08.14.]
[265] Artificial Intelligence Video Interview Act, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68 [2023.08.14.]
[266] 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/ [2023.08.14.]

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

Az Egyesült Királyság például átfogó szabályozási célkitűzéseket tett – többek között – az MI online térben való szabályozás érdekében a 2019-ben publikált „*Online Harms Whitepaper*" elnevezésű dokumentumban, amely célul tűzi ki egy biztonságosabb internet megteremtését, valamint egyes online szolgáltatók felelős megatartását és ennek kapcsán konkrét lépések megtételét, amely kiterjed például a visszaélésekre vagy dezinformáció céljára alkalmazott MI alapú megoldásokra is.[267] A fentieken túl 2023. márciusában az Egyesült Királyság kormánya megjelentetett egy újabb, „*A pro-innovation approach to AI regulation*" elnevezésű dokumentumot,[268] amelyben egyrészt áttekinti a jelenlegi szabályozási helyzetet, valamint az innováció előmozdítását is figyelembe vevő további észrevételeket és javaslatokat tesz az MI szabályozás területén. A dokumentum továbbá konkrét lépéseket is ígér a fentiek megvalósítása érdekében, ideértve – többek között – széleskörű konzultáció 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.[269] Emellett a következő 12 hónapon belül ígéri a dokumentum 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.[270] Mindemellett a fenti dokumentum hosszútávú célokat is meghatároz, ideértve – többek között – egy MI kockázati alapú nyilvántartás, valamint szabályozói homokozó (sandbox) kidolgozását, megjelenítését.[271]

[267] 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 [2023.08.14.]
[268] 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 [2023.08.16.]
[269] A pro-innovation approach to AI regulation [268]. 72-73.
[270] A pro-innovation approach to AI regulation [268]. 73.
[271] Uo.

A fentieken túl az adattovábbítások területén is olyan, általánosnak tekinthető 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 az EU-ból az Egyesült Királyságba történő adattovábbítást megfelelőnek tekintette mind a GDPR által szabályozott,[272] mind a bűnügyi adatvédelmi irányelv[273] által érintett adattovábbítások tekintetében is. 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 fentiekhez hasonlóan, adattovábbítási szempontból Kanadát is megfelelőnek minősítette az Európai Bizottság, közel két évtizeddel korábban, 2001. decemberében meghozott döntésében,[274] 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.[275]

Emellett Japán az elmúlt években szintén jelentős lépéseket tett az adatvédelmi szabályozás területén, amelynek okán az Európai Bizottság 2019-ben meghozott megfelelőségi határozatában megfelelőnek és biztonságosnak ítélte meg az EU-ból Japánba történő adattovábbításokat,[276] amelyek így további adattovábbítással kapcsolatos garanciák megléte

[272] 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, OJ L 360, 11.10.2021, 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)
[273] 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, OJ L 360, 11.10.2021, 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)
[274] 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), OJ L 2, 4.1.2002, p. 13–16 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)
[275] OECD.AI, Pan-Canadian AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-14828 [2023.08.08.]
[276] European Commission, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, 2019.01.23, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 [2023.08.08.]

hiányában is folytathatók. A fentiek mellett Japán szintén 2019-ben hirdette meg saját nemzeti MI stratégiáját,[277] amelynek aktív megvalósítására törekszik, a nemzeti stratégiájában foglalt meghatározásokat és célkitűzéseket pedig évente felülvizsgálja.

A fentiek kapcsán szintén említésre méltó a digitalizációs és MI szabályozás területén a Kínai Népköztársaság, amely az utóbbi időszakban ezen területeken különösen aktívnak bizonyult. Mindez azért is tekinthető lényeges szempontnak, mivel Kína ezeken a területeken eddig a szabályozástól eltekintve 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 pontrendszert és a kormányzat szempontjából nem megfelelőnek ítélt állampolgárok esetleges elvágása bizonyos szolgáltatásoktól (például: repülő- vagy vonatjegy vásárlása).[278] 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 követte pedig egy átfogó MI-t szabályozó törvény, amely várhatóan 2023. második felében jelenik majd meg.[279] A fentiekre tekintettel a technológia és a digitalizáció területén Kína immár nemcsak gazdasági, hanem szabályozói szereplőként is meg kíván jelenni a világgazdaságban.

A fentieken túl Oroszország is meghirdette saját nemzeti MI stratégiáját[280] 2019. végén, az orosz digitalizációs és MI szabályozási megközelítéseket és koncepciókat azonban háttérbe szorította a nyugati hatalmakkal való fokozódó szembenállás és az Ukrajnával vívott háború, amelyek egyben az orosz gazdaság fokozatos elszigetelődéséhez is vezettek.

A fentieken túl természetesen számos egyéb ország alkotott MI fókuszú nemzeti stratégiát vagy vezetett be bizonyos MI fókuszú szabályokat. A fentebb említett, illetve az esetleges egyéb országok szabályozásának bővebb tárgyalása, valamint valamennyi ország szabályozási

[277] OECD.AI, Japan, AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-25312 [2023.08.08.]
[278] Nicole Kobie, The complicated truth about China's social credit system, Wired, Business, 2019.06.07., https://www.wired.co.uk/article/china-social-credit-system-explained [2023.06.07.]
[279] Matt Sheehan, China's AI Regulations and How They Get Made, July 2023, https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf [2023.08.18.]. 9, 24
[280] OECD.AI, Russian Federation, National Strategy for AI Development, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24901 [2023.08.08.]

megközelítésének kifejtése, összevetése azonban túlmutat a jelen mű célkitűzésén és észszerű terjedelmi korlátjain.

d. A digitalizáció és a személyes adatok védelme, a szabályozással kapcsolatos nehézségek

Az MI szabályozásával kapcsolatos kihívások jelentős részben a technológia használatának, eredményeinek, illetve fejlődése, képességei alakulásának előreláthatóságával kapcsolatos nehézségekkel, valamint az MI sokszor csillapíthatatlannak látszó adatéhségével hozhatók összefüggésbe. Az MI által felhasznált adatok azonban sok esetben nem személyes adatok kezelését foglalják magukban, amelyek tekintetében az adatvédelmi jogszabályoknak történő megfelelés sem merül fel, azonban az adatkezelés érinthet személyes, illetve szenzitívnek tekinthető adatokat, valamint különböző adattípusokat egyaránt tartalmazó adatkészleteket is. Mindemellett, ahogy ezt az alább írtakból is láthatjuk, számos esetben nem személyes adatok kezelése is vezethet az érintettek magánélete körébe tartozó, valamint egyéb, szenzitívnek mondható információk felfedéséhez, amely az érintettek számára kiemelt károkat okozhat. Ahhoz azonban, hogy megállapíthassuk az MI általi adatkezelés érintettre gyakorolt hatásait, szükséges annak tisztázása, hogy pontosan milyen adatok sorolhatók a személyes és nem személyes adatok körébe, valamint, hogy az egyes adatok kezelése kapcsán milyen sajátos szempontoknak kell érvényesülniük. Ezt követően szükséges azt is meghatároznunk, hogy az MI általi adatkezelés során milyen típusú adatok kezelése merülhet fel, és ezek hogyan is kapcsolódnak a személyes és nem személyes adatok fenti, általánosnak tekinthető, azaz nem kizárólag MI alapú adatkezelések esetén releváns, csoportosításához. A könnyebb áttekinthetőség kedvéért az egyes, MI alapú adatkezelések által érintett adatokat, adatköröket az alábbi táblázatban foglaltuk össze[281]:

Adatok típusa	Az adatvédelmi jogszabályok hatálya alá tartozik-e?
Személyes adat	Igen

[281] Hangsúlyozandó, hogy az adatok, információk csoportosítása kapcsán számos egyéb szempontrendszer, valamint felosztás elképzelhető.

Szenzitív adat (ideértve a bűnügyi személyes adatokat is[282]	Igen
Közérdekből nyilvános adat	Kizárólag, amennyiben a közérdek által indokolt körön kívül történik adatkezelés
Közérdekű adat	Nem
Egyéb nem személyes adat	Nem, bár közvetetten az érintett azonosítható lehet

Adatvédelmi szempontból a legfontosabb csoportnak a személyes adatok, valamint az azon belül különös védelmet élvező, különleges adatok minősülnek. Ezek védelmére az Európai Unión belül a GDPR, valamint bizonyos esetekben, jellemzően egyes szektorális adatkezelések esetén (például: egészségügyi, foglalkoztatással kapcsolatos adatok vagy banki, fizetési információk) a vonatkozó tagállami jogszabályi rendelkezések is irányadók. 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*”.[283] E tekintetben tehát ugyan tág megfogalmazást alkalmaz a jogszabály, 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. Természetesen, mint ahogy ezt az alábbiakból látni fogjuk, a fentiek nem jelentenek minden esetben egyértelmű támpontot, és csak esetről-esetre állapítható meg, hogy egy adott információ inkább a védendő személyes adatok körébe tartozónak, vagy egyéb információnak tekinthető-e. Hangsúlyozandó azonban, hogy a GDPR technológiasemleges megközelítést alkalmaz,[284] amely többek között a személyes adatok tekintetében is érvényesül, így az új technológiák révén végzett adatkezelések esetén is érvényesül a személyes adatok védelme.[285]

[282] E körbe értve, a GDPR 10. cikkében írtakkal összhangban, „*a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok*” körét.
[283] GDPR 4. cikk 1. pontja
[284] GDPR (15) preambulum-bekezdés
[285] 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

A gyakorlat tükrében akár más személyes adata alapján is azonosítható az érintett, illetve egyéb olyan helyzetek is felmerülhetnek, ahol nem személyes adatok alapján vonatható le az érintettre vonatkozó következtetés. Így például egy 2022-es döntésében az Európai Unió Bírósága („**EUB**") akként foglalt állást, hogy egy adott személy házastársára, illetve élettársára vonatkozó adatok alapján az érintett szexuális irányultságára vonatkozó információk (mint különleges adatok) is levonhatók.[286] Egy másik esetben pedig a brit Adatvédelmi Biztosi Hivatal („*Information Commissioner's Office*"; röviden: „*ICO*") akként foglalt állást, hogy egy kutya neve adott esetben az állat gazdáját is azonosíthatja, így ilyen esetben a kutya neve – bár az önmagában nem lenne személyes adat –, az érintett személyes adatának tekinthető.[287] Ennek kapcsán kiemelendő, hogy az EUB gyakorlata az elmúlt időszakban fokozatosan mozdult el a személyes adat fogalmának relatív értelmezése felé. Ennek kapcsán az EUB a T-557/20. sz. ügyben hozott döntésében különös súllyal vizsgálta anonim adatok vonatkozásában az érintett újbóli azonosításának 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*".[288] Ennek tükrében a jövőben is várhatóan különös hangsúllyal bír majd az érintett azonosíthatósága és az adat személyes adatként való minősülése kapcsán annak vizsgálata, hogy az adatkezelő a birtokában lévő információk alapján képes-e azonosítani az érintettet. Amennyiben ugyanis 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. Ezen megközelítés alkalmazása a digitális gazdaságban és az MI általi adatkezelés esetén is különös jelentőséggel bírhat, tekintettel arra, hogy mind az online térben, mind az MI által kezelt információk jelentős köre anonimizált vagy statisztikai adatokból tevődik össze, amelyek esetén sokszor csak az ezen adatokat elsődlegesen gyűjtő vagy az érintettel közvetlen kapcsolatban álló szolgáltató lehet képes az érintett azonosítására (jellemzően az anonimizálást megelőzően), míg az egyéb szolgáltatók már csak anonimizált, illetve statisztikai adatokhoz vagy egyes technikai

Bernát és Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021. 179-185. 181.

[286] A Bíróság ítélete (nagytanács), 2022. augusztus 1-i, OT kontra Vyriausioji tarnybinės etikos komisija

[287] Freedom of Information Act 2000 (FOIA) Decision Notice, ICO, 2022.02.08, https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4019607/ic-80804-j7c6.pdf. 6.

[288] A Törvényszék T-557/20. sz. ügyben hozott, 2023. április 26-i, Egységes Szanálási Testület v. európai adatvédelmi biztos ítélete 78. bekezdés

információkhoz férnek hozzá, amelyek alapján az egyes további adatkezelők nem képesek az érintetteket azonosítani; ezen esetekben így személyes adatok kezeléséről – az EUB fenti gyakorlatára tekintettel – nem beszélhetünk.

Az álnevesítés, avagy pszeudonimizáció esetén (például: egy adatkészlet kóddal vagy jelszóval való elérhetetlenné tétele illetéktelenek számára) azonban jellemzően személyes adatokról beszélünk, tekintettel arra, hogy ezen adatok képesek az érintettet azonosítani. A gyakorlatban azonban adott esetben kérdésként merülhet fel, hogy személyes adatnak tekinthetők-e az álnevesített adatok akkor is, ha az adatkezelő nem rendelkezik az álnevesítés feloldására szolgáló kóddal, jelszóval, más megoldással vagy eszközzel.[289] A mi részünkről hajlunk arra az álláspontra, miszerint az álnevesített adatok nem tekinthetők személyes adatnak, amennyiben az adatkezelő nem képes az érintett azonosítására, hangsúlyozandónak tartjuk azonban, hogy ezen állapot átmeneti lehet, amennyiben ugyanis az adatkezelő már olyan adat vagy megoldás birtokába jut, amely képes az érintett azonosítására, úgy a vonatkozó adatok személyes adatnak tekinthetők.

Jellemzően sajátos szempontok érvényesülnek az elhunyt személyek adatainak kezelése kapcsán. Ezen személyekkel kapcsolatos adatokra a GDPR ugyan nem terjed ki,[290] azonban a tagállami szabályozás bizonyos szempontból védendőnek minősítheti az elhunytakra vonatkozó egyes információkat vagy dokumentumokat 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 (ideértve az érintett hozzáférési jogát, a helyesbítéshez való jogot, a törléshez való jogot, az adatkezelés korlátozásához való jogot és a tiltakozáshoz való jogot) az érintett által erre kijelölt, illetve meghatalmazott személy jogosult érvényesíteni.[291] Amennyiben ilyen nyilatkozatot az elhunyt életében nem tett, úgy ezen jogokat elsőként gyakorló közeli hozzátartozója[292] ennek hiányában is jogosult a GDPR szerinti adatkezelési műveletek esetén a helyesbítéshez való jogot és a tiltakozáshoz való jogot, valamint jogsértő, illetve az érintett halálával megszűnt adatkezelés

[289] Lásd: EUB, C-413/23 P. felülvizsgálati ügy
[290] GDPR (27) preambulum-bekezdés
[291] Infotv. 25. § (1) bek.
[292] A Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. § (1) 1. pontja értelmében ideértve: „*a házastárs, az egyeneságbeli rokon, az örökbefogadott, a mostoha- és a nevelt gyermek, az örökbefogadó-, a mostoha- és a nevelőszülő és a testvér*”.

esetén a törléshez való jogot és az adatkezelés korlátozásához való jogot érvényesíteni az érintett halálát követő öt éven belül.[293] 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. A fentieken túl szektorális jogszabályi rendelkezések is kiterjeszthetik az adatvédelmi jogszabályi rendelkezések alkalmazását az elhunytak egyes adataira vagy ezeket tartalmazó dokumentumokra. Így például az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 3/A. § szakasza kifejezetten tartalmazza, miszerint „*Az elhunyt személy elhalálozásának körülményeire és a halál okára vonatkozó, valamint az elhunyt személyre vonatkozó egészségügyi dokumentációban foglalt személyes adat kezelésére az egészségügyi adat és az egészségügyi dokumentációban foglalt személyes adat kezelésére vonatkozó kötelező európai uniós jogi aktusban vagy jogszabályban foglalt szabályokat kell alkalmazni*”. A biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 143. § (3) bekezdése szintén kiemeli, miszerint „*e törvény alkalmazásában az elhunyt személyhez kapcsolódó adatok kezelésére a személyes adatok kezelésére vonatkozó jogszabályi rendelkezések az irányadók*”. Így tehát az elhunyt személlyel kapcsolatos fenti adatok és dokumentáció vonatkozásában alkalmazandók a GDPR szabályai, így az ilyen adatok, illetve dokumentáció kezelését végző szervezeteknek ezen követelményt is szükséges figyelembe venniük adatvédelmi megfelelésük során, ideértve azon eseteket is, ha ez elhunyt személyek adatai MI segítségével kerülnek feldolgozásra (például: tudományos kutatások, elemzések végzése során).

Hangsúlyozandó, hogy az esetlegesen irányadó jogszabályi rendelkezésekkel összhangban az egyes személyes adatokat kezelő szolgáltatók saját maguk is jogosultak eljárásrendet bevezetni az elhunytak adatainak kezelése, kiadása, törlése vagy az elhunyt nevében történő eljárás kapcsán, e tekintetben azonban jellemzően jogharmonizációról vagy például a teljes EU-ra kiterjedő átfogó szabályozásról nem beszélhetünk, így e tekintetben a vonatkozó eljárásrend kidolgozása főként az adott közösségi média szolgáltatóra, vagy más online szolgáltatóra

[293] Infotv. 25. § (2) bek.

marad.[294] Erre jó példának tekinthetők az elhunyt személyek közösségi média fiókjának kezelésével kapcsolatos szolgáltatók által követett eljárásrend, illetve gyakorlat.[295] Meggyőződésünk azonban, hogy az idő múlásával párhuzamosan az elhunytakra vonatkozó információk mennyisége is növekedni fog az online térben, ezek, illetve az elhunyt személyek digitális örökségének hatékony kezelése, az érintett családtagok kegyeleti jogainak érvényesítése érdekében szükségessé válhat az EU-n belüli egységes szabályozás kialakítása.

A fentiekhez hasonlóan szintén jellemzően kivételnek tekinthetők a személyes adatok köre alól a jogi személyekre vonatkozó egyes információk. A szervezetekre vonatkozó egyes információk adott esetben azonban szintén tekinthetők az érintettre vonatkozó információnak, bár e tekintetben az EU-n belül egységes és következetes gyakorlatról nem beszélhetünk. A magunk részéről a német 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.[296] Vitatható azonban az ilyen kapcsolat, amennyiben a tag a jogi személy tartozásaiért korlátolt felelősséggel rendelkezik.[297] A fentiekre tekintettel helyesnek tekinthető az olyan gyakorlat kialakulása, amely a korlátlan mögöttes felelősség esetén tekinti az adott szervezetre vonatkozó, főként az adott szervezet gazdasági, szervezeti jellemzőivel kapcsolatos nyilvánosnak nem tekinthető információkat vagy az ilyen egyedüli taggal működő szervezetre vonatkozó gazdasági, megbízhatósággal kapcsolatos értékeléseket személyes adatnak, különösen azon helyzetekben, ahol szoros személyes kapcsolat áll fenn a szervezet és annak egyedüli tagja között (például: egyszemélyes ügyvédi irodák, közjegyzőirodák vagy más egyes

[294] 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 University Press, Edinburgh, 2020. 262-292. 267.
[295] Lásd például a Facebook vonatkozó eljárásrendje és az emlékoldalra vonatkozó szabályok kapcsán: Facebook, Elhunyt személy fiókjának kezelése, https://www.facebook.com/help/275013292838654 [2023.08.15.]
[296] Baden Württemberg Adatvédelmi és Információszabadsági Biztosa („*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 [2023.08.20.] 58., Berlin Adatvédelmi és Információszabadsági Biztosának („*Berliner Beauftragte für Datenschutz und Informationsfreiheit*") 2021. évi éves jelentése, https://www.datenschutz-berlin.de/infothek/publikationen/jahresberichte/ [2023.08.20.] .124-125.
[297] Szászország Adatvédelmi és Információszabadsági Biztosának („*Sächsische Datenschutz- und Transparenzbeauftragte*") 2022. évi éves jelentése, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2022.pdf [2023.08.20.]. 34-36.

egyedüli taggal működő szakmai szervezetek), ezen esetekben ugyanis a fenti adatkezelés egyértelműen azonosítja az egyedüli tagot, valamint alapjaiban kihat annak szakmai megítélésére, megélhetésére is.

Mindemellett különös szabályok vonatkoznak az adott szabályozási környezetben szenzitívnek tekintett adatokra, ideértve például az egészségügyi vagy egyes fizetéssel, hitelbírálattal kapcsolatos adatokat. Az európai uniós szabályozás keretén belül a GDPR az ún. személyes adatok különleges kategóriáinak körébe sorolja

- a faji vagy etnikai származásra,
- a politikai véleményre,
- a vallási vagy világnézeti meggyőződésre, illetve
- a szakszervezeti tagságra utaló, továbbá
- a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatokat,
- az egészségügyi adatokat, és
- a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatokat.[298]

A fenti különlegesnek tekinthető személyes adatok a GDPR tükrében tehát csak meghatározott feltételek teljesülése esetén kezelhetők. Ezen feltételek egyben „többletfeltételnek" is tekinthetők, hiszen a személyes adatok kezelésére irányadó egyéb feltételek (például: adatkezelési cél meghatározása, jogalap megléte, stb.) mellett kell fennállniuk ahhoz, hogy az adott különleges adat kezelhető legyen. Ezen feltételek az alábbiak:

- az érintett kifejezett hozzájárulása a személyes adatok kezeléséhez,
- az adatkezelő vagy az érintett vonatkozásában a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségek teljesítése és konkrét jogok gyakorlása,
- az adatkezelés az érintett vagy más személy létfontosságú érdekeinek védelméhez szükséges (például: az érintett részére életmentő vagy más sürgős egészségügyi ellátás nyújtása céljából),
- alapítványi, egyesületi vagy bármely más nonprofit szervezet tevékenységének keretén belül végzett adatkezelés az adott szervezet tagjai, valamint a vele kapcsolatban álló személyek vonatkozásában,

[298] GDPR 9. cikk (1) bek.

- az érintett által kifejezetten nyilvánosságra hozott személyes adatok kezelése (például: az érintett közszereplése körében vagy közösségi média oldalán nyilvánosan közölt különleges adatok),
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, valamint a bíróságok által igazságszolgáltatási feladatkörben végzett adatkezelés,
- uniós vagy tagállami jogon alapuló jelentős közérdek miatt szükséges adatkezelés (az adott szabályozásra, valamint eseményekre tekintettel ilyenek lehetnek egyes szükségállapot vagy rendkívüli állapot idején végzett, jelentős közérdek miatt szükségessé váló adatkezelések),
- egészségügyi, munkahelyi egészségügyi, illetve munkavégzési képesség felmérése, orvosi diagnózis felállítása, egyes ellátások vagy kezelések megállapítása, egyes egészségügyi, illetve szociális célú adatkezelések,
- népegészségügyi területet érintő közérdek miatt szükségessé váló adatkezelések (például egyes, járvány elleni védekezés céljából végzett adatkezelések),
- uniós vagy tagállami jogon alapuló, közérdekű archiválás céljából, illetve tudományos és történelmi kutatási célból, valamint statisztikai célból szükséges adatkezelések.[299]

Természetesen ezen adatok kezelése tekintetében az egyes nemzeti jogok, valamint az irányadó nemzeti bírósági és hatósági gyakorlat is további feltételeket támaszthatnak, illetve sajátos rendelkezéseket írhatnak elő. Így például jellemzően számos tagállam rendelkezik az egészségügyi adatok kezelésére vonatkozó különös jogszabályi rendelkezésekkel, amelyek a GDPR különleges adatokra irányadó, általánosnak tekinthető követelményein túl, illetve azokkal összhangban érvényesülnek, és veendők figyelembe az ilyen adatokat kezelő személyek, szervezetek által. Különös védelmet élvez továbbá a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok védelme,[300] illetve külön szabályozás irányadó továbbá a bűnügyi adatkezelésekre, amelynek az EU-n belül a bűnügyi adatvédelmi irányelvet[301] átültető tagállami jogszabályok biztosítanak keretet.

[299] GDPR 9. cikk (2) bek. Hangsúlyozandó, hogy a fenti összefoglaló felsorolást a GDPR vonatkozó cikke részletesebben tárgyalja, illetve az egyes feltételek alkalmazhatósága jellemzően az adott eset tükrében vizsgálandó.
[300] GDPR 10. cikk
[301] 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,

Természetesen a fentiekkel ellentétben számos olyan egyéb adat is felmerülhet, amely nem kapcsolható valamely konkrétan meghatározható természetes személyhez (ideértve például: statisztikai adatok, eszközökre vonatkozó vagy egyéb, azonosítható természetes személyekre nem vonatkozó információk). Az ilyen adatok értelemszerűen nem élveznek védelmet adatvédelmi szempontból, azonban gazdasági vagy egyéb okokból hasznosak, illetve értékesek lehetnek, így egyéb jogszabályok lehetnek irányadók az ilyen adatok védelmére, tárolására, megosztására vagy hasznosítására. Megemlítendő azonban, hogy az érintettre vonatkozó információk viszont valóságtartalmuktól függetlenül tekinthetők személyes adatnak, ha azok alapján az érintett azonosítható (ideértve például az érintettet meg nem történt események körében bemutató deepfake felvételeket).

A fentiek körébe tartozhatnak közérdekű adatok[302] is, amelyek nyilvánosságát a törvény közérdekből rendeli el. A közérdekű adatok nyilvánossága egyben a közérdekű feladatokat végző, közhatalmat gyakorló, közpénzekkel gazdálkodó szervezetek transzparens működését is erősítik, továbbá a megfelelő informáltság birtokában ezek ellenőrzését is lehetővé teszik, ekként növelve az államszervezet hatékony működését.[303] Ezen információk jellemzően nem természetes személyekre, hanem közfeladatot ellátó szervezetekre, közpénz kezelésére vagy egyéb, a közérdek számára különös jelentőséggel bíró adatokra, körülményekre vonatkoznak. Amennyiben pedig ezen adatok egy része kapcsán azonosíthatók is természetes személyek (például: közpénzzel gazdálkodó vagy közpénzből származó juttatásban részesülő természetes személyek), ezen esetben a közérdekű adatok nyilvánosságához fűződő érdek jelentősebbnek tekinthető a személyes adatok, illetve – bizonyos mértékig – a személyiségi jogok védelménél. Így például a közhatalmi szereplőknek – a bűncselekményt vagy egyéb súlyos személyiségi jogsértést megvalósító kijelentéseket, megnyilvánulásokat ide nem értve – a közügyek szabad vitatása körében jellemzően tűrniük kell a tisztázatlan, illetve korrupciógyanús ügyekkel

OJ L 119, 4.5.2016, 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

[302] 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).

[303] Komanovics Adrienne, Információszabadság az Európai Unióban, Dialóg Campus Kiadó, Budapest-Pécs, 2009. 13.

kapcsolatos nyilvános kritizálást.[304] E tekintetben azonban az érintett állam alkotmányjogi szempontjai is figyelembe veendők, az esetleges alapjogi összeütközést pedig az adott tagállam területén eljárni hivatott, illetékes bíróság jogosult feloldani.

A fentieken túl szintén nem terjed ki a személyes adatok védelme a közérdekből nyilvános adatokra,[305] amennyiben azok kezelésére azon közérdekkel összhangban kerül sor, amely okán azok nyilvánosságra hozatalra kerültek. Így például egy cég ügyvezetőjének neve és a személyének azonosítására szolgáló alapvető információk a cégnyilvántartásban is közérdekből nyilvános adatként jellenek meg és érhetők el. Ennek célja, hogy az adott cég vezetése, tagsága ellenőrizhető legyen a külvilág számára, az esetleges gazdasági visszaélések pedig elkerülhetők legyenek. Kiemelendő azonban, hogy ezen információk csak a közérdekű céllal összhangban történő kezelésük esetén minősülnek közérdekből nyilvánosnak, más esetekben megtartják „személyes adat" jellegüket. Így egy technológiai nagyvállalat ügyvezetője sem kereshető fel magánelérhetőségein (például: lakcímén vagy magáncélból is használt egyéb elérhetőségein), például egy vállalat számára címzett üzleti ajánlat bemutatása érdekében, tekintettel arra, hogy ez nincs összefüggésben a cégnyilvánossággal és annak közérdekű jellegével kapcsolatban.

Megemlítendő, hogy a közérdekű adatok újrahasznosításával kapcsolatos szabályozás ugyancsak jelentős fejlődést könyvelhetett el az elmúlt időszakban. Ennek kapcsán az európai szabályozás jelentősen megkönnyítette egyes nyílt hozzáférésű adatok, valamint a közszféra információinak újbóli felhasználását, ideértve a sok esetben statisztikai adatokat tartalmazó adatkészleteket, amelyek így könnyebben férhetők hozzá a nyilvánosság számára, és használhatók fel újra.[306] Mindezen adatok újra felhasználását természetesen az MI csak még könnyebbé teszi, tekintettel pedig arra, hogy ezen adatok kapcsán az adatvédelmi jogszabályok nem érvényesülnek, így felhasználásukra is jellemzően rugalmasabban kerülhet sor.

Kiemelendő, hogy az MI általi adatkezelés egyes szakaszai, jellemzői alapján is különböző adatkategóriák különböztethetők meg. Így az MI általi adatkezelés esetén az adatkezelés

[304] Ligeti Miklós, A közérdekű adatok megismerhetőségének buktatói, Infokommunikáció és jog, 2015/1. 26-30. 27.

[305] 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).

[306] Lásd: az Európai Parlament és a Tanács (EU) 2019/1024 irányelve a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

folyamatának lépései alapján alapvetően bemeneti („*input*”) és kimeneti („*output*”) adatokat különböztethetünk meg, amelyeket az MI alkalmazás 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*”).[307]

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. Az adatvédelmi jogszabályi rendelkezéseken túl továbbá egyéb jogszabályi rendelkezések is alkalmazhatók lehetnek az MI által kezelt adatokra, adatkészletekre vonatkozóan, ideértve például a szellemi tulajdonjogi, valamint személyiségi jogok védelmével kapcsolatos jogszabályi rendelkezéseket. A fentiekre tekintettel tehát, amennyiben akár a bemeneti, akár a kimeneti vagy az adatkezelés folyamata során kezelt adatok személyes adatoknak minősülnek, legalább ezen személyes adat kezelésével járó folyamat-szakaszra vonatkozóan az adatvédelmi elvárások és jogszabályi követelmények irányadók lesznek. Természetesen ez egyéb jogszabályi követelményeknek való esetleges megfelelés ezen felül is irányadó lehet. Így például, ha az adott megoldás szerzői jogilag védett információt kezel, úgy e tekintetben szükséges az üzemeltetőnek vagy felhasználónak a szerzői jogi jogszabályi követelményeknek való megfelelést is biztosítania.

A fentiekre tekintettel megállapítható, hogy az MI általi adatkezelés kapcsán elsődlegesen az adatok típusa vizsgálandó, olyan esetekben ugyanis, ha nem személyes adatok kezelése történik, úgy az adatvédelmi jogszabályi rendelkezések sem érvényesülnek. Természetesen azonban az adat esetleges személyes adat jellege kapcsán számos esetben csak esetről-esetre dönthető el, hogy sor kerül-e személyes adatok kezelésére, amennyiben pedig igen, úgy milyen szempontok, illetve feltételek szerint.

4. A mesterséges intelligencia általi adatkezelés az Európai Unióban

[307] Dario Casella, Laurence Lawson, AI and privacy: Everything you need to know about trust and technology, ericsson.com, 2022.08.01, https://www.ericsson.com/en/blog/2022/8/ai-and-privacy-everything-you-need-to-know [2023.05.14.]

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 szerepet kap. Segítségével például számos információt könnyebben megtalálhatunk, korábban soha nem látott módon fejezhetjük ki magunkat, vagy az eddigieknél jóval gyorsabban végezhetünk el számos hétköznapi feladatot (például: információk könnyebb rendszerezése, beosztása, hétköznapi ügyintézés támogatása). Az MI által nyújtott mindezen előny azonban a személyes adatok nagyobb fokú kezelésével is jár, és számos területen egyéb társadalmi szempontból jelentős kockázatokkal is járhat, amelyet az európai jogalkotás is igyekszik megfelelő módon kezelni, ideértve különösen az etikus MI-felhasználás keretrendszerének meghatározását, valamint az MI felhasználásával kapcsolatos felelősség észszerű és arányos elosztását.

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, tekintettel arra, hogy az MI elsődleges „tápanyagának” az adat tekinthető, amely révén az MI képes eredményt produkálni, 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. Emellett a jelen fejezetben az MI általi adatkezelés egyéb jelentős szempontjai is összefoglalásra kerülnek, ideértve például az adatvédelmi hatásvizsgálat vagy a hatósági ellenőrzés szempontjait, valamint a szektorális adatkezeléssel kapcsolatos egyes kihívásokat. Ennek kapcsán – a tanulmány terjedelmi kereteire tekintettel – az MI valamennyi iparág, illetve szakterület kapcsán végzett alkalmazásának adatvédelmi szempontjai ismertetésétől értelemszerűen eltekintettünk, és a társadalom működése szempontjából kiemelt fontossággal bíró területekre, így az egészségügyi, valamint a munkahelyi adatkezelésre és az MI online platformokon való alkalmazására fókuszáltunk. Természetesen az MI alkalmazását és annak adatvédelmi szempontjait számos területen jelentősnek tartjuk (ideértve például: a közlekedést, az ipari célú vagy a szociális interakciók

céljából végzett alkalmazást), azonban igyekeztünk olyan szektorális szempontokat megragadni, amelyek különösen közeli kapcsolatba hozzák az MI-t az emberrel, és társadalmi szempontból is kiemelt jelentőséggel bírnak. Ennek kapcsán azonban a tanulmány egyéb részeiben az MI egyéb területeken való alkalmazásával is foglalkozunk, valamint alább külön fejezetben tárgyaljuk a digitalizáció és az adatvédelem további kihívásait, amelyek területén az adatvédelmi elvárások a közeljövőben vélhetőleg egyre nagyobb hangsúllyal bírnak majd.

a. 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 adatkezelés jellemzően nagy mennyiségű személyes adatot érint, kiterjedt, sok esetben nehezen átlátható, valamint sokszereplős. Az egyes szerepkörök meghatározásával kapcsolatos bizonytalanságok azonban mind az érintettek, mind az adatkezelésben résztvevők számára jelentős kihívást jelentenek. Erre tekintettel szükséges az egyes szerepköröket az adatkezelésben résztvevőknek még annak megkezdése előtt tisztáznia, valamint az érintettek felé is ennek megfelelően megjelenni.

Ennek kapcsán kiemelendő, hogy a személyes adatok kezelése során adatkezelőnek az a személy vagy szervezet tekintendő, amely az adatkezelés céljait és eszközeit önállóan vagy másokkal együtt meghatározza,[308] míg adatfeldolgozónak tekintendő az a személy vagy szervezet, amely az adatkezelő nevében személyes adatokat kezel.[309] A GDPR külön rendelkezéseket tartalmaz továbbá a közös adatkezelőkre vonatkozóan is, amelyek az adatkezelés céljait és eszközeit közösen határozzák meg.[310] 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 vagy közös

[308] GDPR 4. cikk 7. pontja
[309] GDPR 4. cikk 8. pontja
[310] GDPR 26. cikk

adatkezelőnek, sem pedig adatfeldolgozónak a munkáltatója nevében eljáró munkavállaló, ennek adatkezeléssel járó tevékenysége ugyanis az őt alkalmazó adatkezelőnek tudható be.[311]

Hangsúlyozandó azonban, 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 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.[312] Így amennyiben egy ügyvédi iroda például egy ügyféllel szembeni hatósági eljárás kapcsán, a megbízás keretén 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. Hasonló helyzetről beszélhetünk például orvosok esetén is, akik a rájuk irányadó szakmai és etikai szabályokra tekintettel járnak el, valamin az alábbiak szerint a könyvelők esetén is.[313]

Bizonyos esetekben azonban kérdéses lehet, és jellemzően csak esetről-esetre dönthető el, hogy az adott szolgáltató adatkezelőnek vagy adatfeldolgozónak tekinthető-e. Részben a fenti példánál maradva a könyvelő vagy könyvelőiroda jellemzően a megbízói utasítások függvényében minősül adatkezelőnek vagy adatfeldolgozónak; amennyiben a megbízó részletes utasításokat tesz, amely például az adatok vagy érintettek kategorizálására, az adatkezelés megszervezésének szempontjaira is kiterjed, úgy a könyvelő adatfeldolgozónak tekinthető, amennyiben azonban általános jellegű megbízás keretén belül, jellemzően saját szervezése, döntései mentén jár el a könyvelő, úgy adatkezelőnek tekinthető.[314]

---

[311] 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. [2023.09.11.]
[312] 07/2020. sz. iránymutatás az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról („**07/2020. sz. Iránymutatás**”) 14.
[313] 07/2020. sz. Iránymutatás, 17.
[314] Uo.

A fenti szerepkörök azonban számos esetben nem különíthetők el ilyen könnyen, és sok esetben egy adott személy vagy szervezet egymással szoros kapcsolatban álló adatkezelések esetén 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, illetve az ezekkel való szerződés fenntartása is az adott tag érdeke, 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. Jellemzőnek tekinthető továbbá, hogy egy-egy szolgáltatás- vagy tevékenységtípus vegyesnek tekinthető adatkezeléssel kapcsolatos szerepkörökhöz vezethet. Fejvadászok vagy hasonló toborzást támogató vállalkozások például sok esetben a jelöltet kereső munkáltatói ügyfeleikkel közös adatkezelőnek minősülnek, a felek a saját adatbázisaik üzemeltetése és későbbi saját célú adatkezeléseik (például: a munkáltató által végzett, a jelölt sikeres felvételét követő munkahelyi adatkezelés) során önálló adatkezelőként, egymástól függetlenül járnak el.[315]

Természetesen az adatkezeléssel kapcsolatos szerepek tükrében a feleknek a megfelelő megállapodást kell kötniük egymással. Így a közös adatkezelőknek a közös adatkezeléssel kapcsolatos megállapodást szükséges kötniük, a megállapodás lényegét pedig szükséges összefoglalniuk, az adatkezeléssel kapcsolatos szerepek és felelősség egyértelmű meghatározásával, a fenti összefoglalást pedig az érintett rendelkezésére kell bocsátaniuk.[316] Így amennyiben két kutatóintézet közösen végez kutatást MI alapú megoldás alkalmazásával, úgy a résztvevőknek szóló adatvédelmi tájékoztatóban szükséges meghatározni a közös adatkezelőket, valamint egyértelműen tükrözni szerepüket és az általuk végzett adatkezelési tevékenységeket (például: adatvédelmi, vizsgálat elvégzése, kiértékelése, 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

[315] 07/2020 sz. Iránymutatás, 25-26.
[316] GDPR 26. cikk (2) bekezdés

kutatás céljára használható), úgy az ennek megfelelő szerződést szükséges a feleknek megkötniük a GDPR-ban meghatározott tartalmi elemekkel.[317]

b. A mesterséges intelligencia és az átláthatóság

Az átláthatóság alapvető adatvédelmi követelménynek tekinthető, lehetővé téve, hogy az érintettek tudomást szerezzenek személyes adataik kezeléséről. Az átláthatóság biztosítása erre tekintettel az európai adatvédelmi jogban, így különösen a GDPR-ban is az adatkezelő egyik alapvető kötelezettségeként, valamint alapelvként jelenik meg.[318] Ennek tükrében a személyes adatok kezelésével kapcsolatos tájékoztatásnak, illetve kommunikációnak könnyen hozzáférhetőnek és közérthetőnek kell lennie, valamint az adatkezelőnek azokat világosan és egyszerű nyelvezettel szükséges megfogalmaznia,[319] hogy azt az érintettek megérthessék.

A fentiekre tekintettel például elengedhetetlen, hogy az érintetteknek szóló adatvédelmi tájékoztató az érintettek által értett nyelven íródjon. Átlag fogyasztók esetén például közismert kifejezések, a köztudatban jelen lévő fogalmak, 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 nem érthető.[320]. Szakértők részére szóló tájékoztató esetén azonban alkalmazhatók az adott szakterületen alkalmazott, az adott szakértők által jellemzően ismert szakkifejezések. Így például egy orvosi, kutatói személyzet számára szóló adatvédelmi tájékoztatóban használhatók orvosi kifejezések (például: egyes eljárások, vizsgálattípusok kapcsán történő adatkezelésekről való tájékoztatás). 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 általános jellegű volt, több esetben technikai szakszavakat használt, valamint kizárólag angolul volt elérhető. Kiemelendő azonban, hogy a szankció alkalmazása során a hatóság alacsony szintűnek tekintette a fenti jogsértést, figyelembe vette azonban a Spotify bevételét, valamint az érintett felhasználók nagy számát. A hatóság továbbá a cég

[317] GDPR 28. cikk (3) bekezdés
[318] GDPR 5. cikk (1) a) pontja
[319] GDPR (39) preambulum-bekezdés
[320] NAIH/2015/2201/17/H, https://www.naih.hu/files/NAIH-2015-2201-H_hatarozat.pdf [2023.05.04.]. 30.

érintettek hozzáférési joga gyakorlásának kezelésével kapcsolatos gyakorlata vonatkozásában nem állapította meg jogsértést, ezt az alább írtak szerint megfelelőnek tekintette.[321]

Az adatkezelés során a gyermekek személyes adatai különös védelmet érdemelnek, mindez pedig az adatkezelésről szóló tájékoztatás kapcsán is jelentős hangsúllyal 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.[322] Emellett a gyermekek jellemzően befolyásolhatóbbak mint felnőtt társaik, így a gyermekeket célzó egyes adatkezelések, különösen a marketing célú megkeresések vagy egyes online szolgáltatásokkal, közösségi médiával kapcsolatos adatkezelési műveletek kapcsán kiemelten fontos az adatkezelés átláthatóságának biztosítása,[323] ideértve az adatkezelésről, valamint az érintetti jogokról való tájékoztatást is. Erre tekintettel az olyan adatkezelések vonatkozásában, amelyek kifejezetten gyermekekre vonatkoznak, a tájékoztatást olyan nyelven kell megfogalmazni, amelyet az adott korosztályba tartozó gyermekek könnyen megérthetnek.[324] A nemzetközi gyakorlatból például jó példának tekinthető az Egyesült Nemzetek Szervezetének („**ENSZ**”) gyermekek jogairól szóló egyezményének gyermekbarát szövege, amely az ENSZ weboldalán is elérhető.[325] Ennek kapcsán tehát hangsúlyozandó, hogy egy fentiek szerinti, gyermekeknek szóló adatvédelmi tájékoztatóban halmozottan kerülni kell az olyan kifejezéseket, szófordulatokat, amelyek a közbeszédben nem számítanak elterjedtnek, illetve nem köztudomásúak, és emellett is olyan nyelvezet alkalmazandó, amelyet egy gyermek is megérthet (például: a komplex, elvont fogalmak helyett köznapi, egyszerű megfogalmazások). E körben több játékok gyártásával, forgalmazásával foglalkozó cég is készített és publikált már adatvédelmi tájékoztatót, akár az európai, akár az amerikai adatvédelmi követelményekre tekintettel, ideértve például a Lego vállalatot (amely egy adatkezeléseit, valamint az érintettek jogait gyermekek részére játékosan

[321] Svéd adatvédelmi hatóság (“*Swedish Authority for Privacy Protection*”), Administrative fee against Spotify, megjelent: 2023.06.13, https://www.imy.se/en/news/administrative-fee-against-spotify/ [2023.07.18.]
[322] GDPR (38) preambulum-bekezdés
[323] Uo.
[324] GDPR (58) preambulum-bekezdés
[325] 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 [2023.05.07.], 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.

bemutató videót is közzétett a weboldalán),[326] vagy a Barbie babákat gyártó Mattel vállalatot (amely utóbbi a gyermek törvényes képviselőjét szólítja meg).[327]

Természetesen a gyakorlatban kérdésként merülhet fel, hogy mi tekinthető „*kifejezetten gyermekekre vonatkozó adatkezelésnek*”.[328] Ez azonban értelemszerűen csak esetről-esetre határozható meg. Az olyan üzletekben, webáruházakon keresztül, illetve szolgáltatások, termékek kapcsán végzett adatkezelések esetén, amelyek jellemzően gyermekekre vonatkoznak, általában véve kifejezetten gyermekekre vonatkozónak tekinthetünk. Így például egy játékbolt webáruháza, egy gyermekkórház vagy egy óvoda által a gyermekek vonatkozásában végzett adatkezelés is ilyennek tekinthető. Vélhetőleg szintén ilyennek tekinthetők az olyan adatkezelések is, amelyek egy-egy szolgáltatáshoz vagy termékhez kapcsolódóan gyakran más korosztályok képviselőire is vonatkoznak, ha a gyermekek mint érintetti csoport az adott szolgáltatás vagy termékkör jellemző címzettje, illetve, ha a közvélekedés is a gyermekeket gyakran ezen szolgáltatások vagy termékek jellemző igénybe vevői, használói közé sorolja. Ilyennek tekinthető például egy számítógépes játékokat forgalmazó webáruház, hiszen bár ilyen játékokkal gyakran felnőttek is szívesen játszanak, a gyermeki felhasználók esetükben felülreprezentáltnak tekinthetők. Kérdéses azonban, hogy például egy bevásárlóközpont vagy szupermarket által végzett adatkezelés (például: kamerarendszer működtetése vagy áruforgalmazási tevékenysége során végzett adatkezelés) esetén ez a logika alkalmazható-e, hiszen ezek területén is gyakran találunk gyermekeket. Mivel azonban ezek üzemeltetői a fenti területeket jellemzően a társadalom széles köre számára teszik elérhetővé, illetve az itt folytatott kereskedelmi tevékenység is jellemzően valamennyi potenciális vásárló felé általános jelleggel irányul, így az ezek kapcsán folytatott adatkezelések jellemzően nem tekinthetők kifejezetten gyermekekre vonatkozónak. Megemlítendő azonban, hogy egy szupermarket vagy egy bevásárlóközpont egyes területei, illetve az itt végzett egyes tevékenységek kapcsán is felmerülhetnek olyan adatkezelések, amelyek – ezen területek, egységek, tevékenységek kapcsán – kifejezetten gyermekekre vonatkozónak tekinthetők (például: a bevásárlóközpont területén található játszóház, gyermekmegőrző vagy játékbolt kapcsán végzett adatkezelések).

[326] Lego, Now some serious stuff, https://www.lego.com/en-us/kids/legal/privacy-policy-short [2023.09.11.]
[327] Mattel Children's Privacy Statement, https://shop.mattel.com/pages/childrens-privacy-statement [2023.09.11.]
[328] GDPR (58) preambulum-bekezdés

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. Természetesen azonban, ha a gyermek a fenti információk megértésére, befogadására fejlettségére, állapotára tekintettel nem képes (például: csecsemők vagy adott esetben értelmi fogyatékos gyermekek esetén), úgy elegendő a nevükben eljáró személyek részére megadni a tájékoztatást, hiszen ilyen esetben a kifejezetten gyermek részére címzett tájékoztatás értelmetlen lenne vagy zavaróan hatna.

A fentiek szerint, tehát, amennyiben egy gyermek egészségügyi dokumentációját használják fel egy egészségügyi MI alkalmazás fejlesztéséhez, és a gyermek részére megfelelő tájékoztatás nyújtható személyes adatai kezeléséről, úgy szükséges röviden a részére is összefoglalni, hogy az adatai gyűjtése és felhasználása miért szükséges, illetve milyen hatásokkal járhat (például: a gyógyulására vagy más személyek gyógyulására hatással lehet-e, ennek kapcsán milyen adatait gyűjtik, milyen jogai lehetnek). Ilyen esetben is 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 dönt az adatkezelésről. Ilyen esetekben helyesebb lehet a tájékoztatást is kizárólag a törvényes képviselőnek címezni az esetleges károk, a gyermekre nehezedő emocionális, illetve pszichológiai megterhelés elkerülése érdekében. Olyan esetekben továbbá, ahol az adatkezelő a gyermekkel egyáltalán nem kerül kapcsolatba, jellemzően szintén alappal hivatkozhat arra, hogy a tájékoztatást elegendő a szülőnek vagy más törvényes képviselőnek címeznie, és a felnőttek által értett nyelven megfogalmaznia, hiszen itt a gyermek kizárólag a szülő vagy a törvényes képviselő által szerezhet tudomást az adatkezelésről, valamint akaratát – a lehetséges mértékben – csak rajta keresztül érvényesítheti.

A gyermekek adatai védelmének fontossága természetesen nem hangsúlyozható eléggé, a kérdés pedig az adatvédelmi hatóságok számára is egyre jelentősebb fókuszt képez. Így az ír adatvédelmi hatóság 2023. szeptemberében 345 millió eurós adatvédelmi bírsággal sújtotta a TikTok-ot, tekintettel arra, hogy az alkalmazás számos tekintetben jogsértő módon kezelte a gyermekkorú felhasználók személyes adatait. Így a gyermekkorú felhasználók profilja például automatikus módon publikusra volt állítva, a „Family Pairing” nevű funkció segítségével pedig

a gyermekkel ellenőrizetlen felnőttkorú személyek léphettek kapcsolatba. Ezentúl a hatóság különös súllyal vette figyelembe annak tényét, hogy a TikTok nem nyújtott átlátható tájékoztatást a felhasználók részére, valamint olyan sötét mintákat alkalmazott a regisztráció, valamint a videótartalmak feltöltése során, amelyek alacsonyabb adatvédelmi szintet jelentő beállítások elfogadására késztették a felhasználókat.[329]

Természetesen egyéb sérülékeny csoportok kapcsán is sajátosan érvényesülhet a tájékoztatás követelménye. Ennek kapcsán érdemes megemlíteni, hogy 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.[330] Emellett is lehetőség van továbbá a tájékoztatás és az azt segítő ikonok vizualizálására, például QR kódok vagy rövidebb tájékoztatóanyagok útján,[331] de akár az adatkezelés által indokoltak szerinti egyéb formátumban vagy módon is (például drónok által megfigyelt területen tábla kihelyezésével, illetve nyilvános tájékoztató kampányok útján).[332]

A fenti tájékoztatással kapcsolatos gyakorlati megoldások az adatkezelés céljából alkalmazott technológia vagy alkalmazás által érintett szélesebb rétegeken túl sok esetben a fogyatékkal élő vagy életkoruk, egészségügyi állapotuk okán más szövegezésű vagy eltérő formátumú információ befogadására képes személyek számára különös segítséget nyújthatnak. 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. 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. Ha pedig a tájékoztatást idegen nyelvű személyeknek

[329] Irish Data Protection Commission announces €345 million fine of TikTok, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok#:~:text=The%20Data%20Protection%20Commission%20(DPC,TTL)%20on%201%20September%202023. [2023.09.17.]
[330] GDPR 12. cikk (7) bekezdés
[331] Átláthatósággal kapcsolatos Munkacsoport Vélemény, 27-28.
[332] Átláthatósággal kapcsolatos Munkacsoport Vélemény, 24.

is nyújtják, és a tájékoztató lefordításra kerül, azt következetes módon, illetve az adott nyelven is közérthetően szükséges megtenni.[333]

A tájékoztatással kapcsolatos fenti kihívásokon túl az MI általi adatkezelés kapcsán gyakran merül fel az ún. fekete-doboz probléma, amely szerint az alkalmazott modell olyan eredményekhez is vezethet, amelyek előre nem láthatók, így a személyes adatok kezelésének pontos hatásai, az ezek felhasználásával születő döntések sem láthatók teljes mértékben előre az adatkezelő által.[334] Ennek kapcsán a GDPR is alapvető követelményként határozza meg az érintettek automatizált döntéshozatal, illetve a profilalkotás[335] tényéről való tájékoztatását, valamint azon információk rendelkezésükre bocsátását, hogy az adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.[336] Így tehát az érintetteknek át kell látniuk az adatkezelés jelentőségét, helyzetükre, illetve jogaikra és szabadságaikra gyakorolt hatásait, azonban ez nem terjed ki szükségszerűen valamennyi lehetséges döntésre, és valamennyi potenciális döntésre, eredményre, kizárólag azok típusára, az érintettekre gyakorolt jellemző hatásokra, vonatkozó kockázatokra. Mindez egyben segítséget nyújt az érintett számára, hogy felmérje 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 tájékoztatás a fentiek tükrében is gyakran kihívást jelenthet, ideértve azon eseteket, ahol az alkalmazott technológia, illetve az adatkezelési művelet különösen összetettnek tekinthető, vagy ha az érintetti csoport sajátos tájékoztatási igényekkel bír, illetve szenzitívnek tekinthető.[337] Ilyen esetekben tehát az adatkezelőknek különös gondot kell fordítaniuk az adatkezelésről való megfelelő tájékoztatás nyújtására.

---

[333] Átláthatósággal kapcsolatos Munkacsoport Vélemény, 10.
[334] Datatilsynet, Artificial intelligence and privacy, Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [2023.04.20.]
[335] 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*".
[336] GDPR 13. cikk (2) f) pontja, 14 cikk (2) g) pontja
[337] Necz Dániel, Az adatkezelésről való tájékoztatás technológiai környezetben, különös tekintettel az Egyesült Államok szabályozására, Jogi Fórum, 2022, https://www.jogiforum.hu/wp-content/uploads/2022/09/necz-daniel_adatkezelesrol-valo-tajekoztatas-technologiai-kornyezetben_cimlappal.pdf [2023.09.17.]. 11.

Az adatvédelmi hatósági gyakorlat is egyre nagyobb hangsúlyt helyez az automatizált döntéshozatalra, illetve a profilalkotásra, valamint azok átlátható végzésére. 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.[338]

Az átláthatóság problémája az online térben külön kihívást jelent továbbá a marketing szolgáltatások területén, ahol jellemzően számos vállalkozás és szolgáltató továbbít egymásnak, sok esetben profilalkotás útján nyert, fogyasztói viselkedéssel kapcsolatos információkat, majd jellemzően ez alapján keresik meg a fogyasztókat célzott reklámtartalmakkal. Az adatok forrása, további feldolgozása, valamint az adattovábbítások láncolata azonban sok esetben átláthatatlan az érintettek számára, amelyet az adatvédelmi hatósági gyakorlat is több esetben kifogásolt már az EU-n belül. A francia adatvédelmi hatóság például 2023-ban 40 millió eurós adatvédelmi bírsággal sújtotta a CRITEO elnevezésű, online marketing területén aktív céget, amely jellemzően a fogyasztói online viselkedés (például: webshopon keresztüli vásárlás) értékelése alapján nyújt marketing szolgáltatásokat. Az eset során az adatvédelmi hatóság különös súllyal értékelte többek között a CRITEO adatkezelésének átláthatatlanságát, valamint adatvédelmi tájékoztatójának általános, nehezen megfogható nyelvezetét.[339]

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 a fentiek révén hajlítják (például: bizonyos információk elhallgatásával vagy kiemelésével).[340] A sötét megoldások többféle szempont alapján csoportosíthatók, illetve

[338] Berlin Adatvédelmi és Információszabadsági Biztosa, Computer sagt Nein, 2023.05.31, https://www.datenschutz-berlin.de/pressemitteilung/computer-sagt-nein/ [2023.08.20.]
[339] CNIL, Personalised advertising: CRITEO fined EUR 40 million, 22 June 2023, https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million [2023.08.21.]
[340] 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.

többféle kategóriába sorolhatók. Az Európai Adatvédelmi Testület („**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;
- 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.[341]

A fentebb írtak szerint 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.[342] 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 az ellentmondásos kifejezések és információk („*ambiguous wording or information*”) alkategóriákat különbözteti meg.[343]

[341] EDPB 3/2022. sz. Iránymutatása, 7-8.
[342] Domokos Márton, Horváth Anna Zsófia, Dark patterns – napvilágra kerülő sötét megoldások, Jogi Fórum, https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/ [2023.06.16.]
[343] EDPB 3/2022. sz. Iránymutatása, 63-64.

A fentiekre tekintettel a sötét minták az MI kapcsán is különös jelentőséggel bírhatnak, tekintettel arra, hogy az MI a fenti megoldások alkalmazásával még hatékonyabb módon lehet képes az érintettek befolyásolására (például: meghatározott információk elhallgatásával, felnagyításával vagy elferdítésével). Így például az MI hatékonyan tüntethet fel jelentéktelennek vagy épp hangsúlyosabbnak bizonyos információkat, vagy akár hamis információkkal is manipulálhatja az érintettet. Ez különösen igaz lehet a különböző chatbot alkalmazásokra, amelyek hatékonyan és meglepő rugalmassággal képesek a felhasználók megkereséseire reagálni, illetve a válaszokat a felhasználók elvárásaira, igényeire szabni.

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.[344] 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.[345]

A tájékoztatás kötelezettsége alól azonban kivételek is meghatározhatók, ideértve különösen azon eseteket, amennyiben az érintett már rendelkezik a tájékoztatás körébe tartozó információkkal.[346] Így tehát, amennyiben az érintett már korábban tudomást szerzett arról, hogy személyes adatait MI alapú megoldás alkalmazásával kezelik (például: toborzás támogatása céljából), úgy ennek kapcsán a körülmények változatlansága esetén szükségtelen az érintettet (újból) tájékoztatni. 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.[347] Amennyiben tehát történelmi kutatás céljából MI megoldás alkalmazásával végzik évtizedekkel

[344] GDPR 13. cikk (1) bek.
[345] GDPR 14. cikk (3) bek.
[346] GDPR 13. cikk (4) bek., GDPR 14. cikk (5) bek. a) pontja
[347] GDPR 14. cikk (5) bek. b) pontja

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.[348] Az egyházak általi adatkezelés – az adott egyház eljárásrendjét és szokásait is figyelembe véve – megköveteli a hívekkel való interakció sajátosságainak figyelembevételét az érintetti jogok gyakorlásának támogatása során is (ideértve például: gyónási vagy más hasonló titok figyelembevétele).[349] Így amennyiben sor is kerül bizonyos esetekben az MI egyházak általi alkalmazására (például: az egyházi szervezet weboldalán chatbot segíti a webodalon való tájékozódást), úgy ennek kapcsán mind az irányadó adatvédelmi jogszabályi rendelkezéseket, mind az adott egyház szabályait és elvárásait szükséges lehet adott esetben betartani.

c. A mesterséges intelligencia általi adatkezelés jogalapja és jogszerűsége

Az MI általi adatkezelés jogszerűsége a megbízható MI alkalmazása szempontjából kiemelt jelentőséggel bír. Az MI szabályozásával kapcsolatos alapelveket, valamint a technológiával kapcsolatos etikai szempontokat a tanulmány korábbi fejezeteiben már tárgyaltuk,[350] így a jelen fejezetben kifejezetten az MI általi adatkezelés jogszerűségére, valamint a megfelelő jogalapok hivatkozására fókuszálunk.

Az MI általi adatkezelés jogszerűsége kapcsán az EU-n belül kiemelt jelentőséggel bír a GDPR-ban meghatározott, személyes adatok kezelésére vonatkozó elveknek 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”),

[348] GDPR 14. cikk (5) bek. c-d) pontjai
[349] Necz Dániel: Az egyházak általi adatkezelés. In: Kiss Gábor (szerk.): Fiatal Kutatók és Doktoranduszok X. Nemzetközi Jubileumi Teológus-Konferenciájának Tanulmánykötete, Doktoranduszok Országos Szövetsége, Budapest, 2020. 422.
[350] Lásd: A tanulmány 2. c, valamint 2. d. iii. pontjaiban írtak.

- 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”).[351]

A fentiek mellett a GDPR kiemeli, miszerint az adatkezelő felelős a fenti alapelveknek való megfelelésért, valamint képesnek kell lennie a megfelelés igazolására („elszámoltathatóság”),[352] így utolsó alapelvként szerepeltetve az alapelveknek való megfelelő adatkezelést és annak szükség szerinti igazolását.

A fenti alapelveknek értelemszerűen az MI általi adatkezelés kapcsán is érvényesülniük kell. Így a jogszerű és tisztességes eljárás és átláthatóság alapelvi követelményeire tekintettel az adatkezelőtől a tételes jogszabály-követésen túl elvárható az adatkezeléssel járó kockázatok előzetes felmérése (különös adatvédelmi hatásvizsgálat keretében), azok kiküszöbölésére vagy csökkentésére szolgáló megfelelő intézkedések alkalmazása, és az érintett tájékoztatása annak érdekében, hogy az adatkezelésre és annak hatásaira, kockázataira megfelelően felkészülhessen.[353] 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 célhoz szükséges adatkört, valamint szervezi meg az adatkezelést.[354] Az MI általi adatkezelés esetén 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 az adatkezelés egyes szakaszait is akként szükséges meghatároznia az MI általi adatkezelést

[351] GDPR 5. cikk (1) bek.
[352] GDPR 5. cikk (2) bek.
[353] Necz Dániel: A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai. Acta Humana – Emberi Jogi Közlemények, 10(3), 95–123. https://doi.org/10.32566/ah.2022.3.4. 101.
[354] Révész Balázs, Az adatkezelés alapelvei. In: Péterfalvi Attila, Révész Balázs, Buzás Péter, Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., Budapest, 2021. 103-121. 105.

folytatóknak, hogy az érintettek csak a szükséges ideig maradjanak azonosíthatók, míg az adatkezelés későbbi vagy egyéb szakaszaiban az adatkezelés anonimizált (például: statisztikai adatok) módon is végezhető. Megjegyzendő azonban, hogy a kezelt adatok naprakészsége, habár 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.[355] 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, amelyek így akarva-akaratlanul a későbbi eredmények során, más felhasználóknál is felbukkanhatnak.[356]

Természetesen az MI általi adatkezelés kapcsán egyéb, jellemzően szektorális jogszabályok, szabályozott szakmák vagy más területek alapelvei, egyéb szokások, értékek vagy célkitűzések is relevánsak lehetnek, az MI EU-n belüli alkalmazása kapcsán azonban a fenti alapelveknek történő megfelelés kiemelt jelentőséggel bír. Így az MI általi adatkezelés esetén is kiemelten fontos az adatkezelés irányadó jogszabályi rendelkezésekkel, szakmai szabályokkal és iránymutatásokkal, valamint etikai elvárásokkal összhangban történő, átlátható végzése, valamint az adatkezelés céljának megfelelő, a gyűjtött és feldolgozott adatok szempontjából takarékos módon végzett adatkezelés, amelyhez az adatkezelés formájának is idomulnia kell, az adatkezelőnek pedig megfelelő szervezési és technikai intézkedéseket kell alkalmaznia az adatok védelme érdekében.

Sajátos módon érvényesül a pontosság elve az MI általi adatkezelés esetén, tekintettel arra, hogy számos esetben a hibás vagy elavult adatok további kezelése vagy megőrzése is az MI tanulási, fejlesztési folyamatának részét képezheti, illetve az esetleges hibák azonosítása szempontjából is kiemelt jelentőséggel bírhat.[357]

[355] Necz [353]. 102-103.
[356] 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/ [2023.09.15.]
[357] Necz [353]. 102-106.

Természetesen az MI általi adatkezelés esetén a fenti elveknek való megfelelésen túl szükséges a megfelelő jogalap megválasztása is. 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.[358]

A személyes adatok kezelése tehát az EU-n belül a fenti jogalapok valamelyike szerint történhet, amely az MI általi adatkezelések esetén is irányadó. Az adatkezelés egyik igen gyakran idézett jogalapjaként a hozzájárulás[359] tekinthető, amelynek megfelelő hivatkozása esetén azonban több feltételnek is teljesülnie kell. Így a hozzájárulásnak

- önkéntesnek,
- konkrétnak,
- tájékoztatáson alapulónak, és
- egyértelműnek

kell lennie.[360] 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,[361] amelyet jellemzően kizár, többek között, az egyenlőtlen viszonyban, kényszer vagy szankciótól való félelem hatására adott hozzájárulás, illetve a szükségtelenül

[358] GDPR 6. cikk
[359] GDPR 6. cikk (1) a) pontja
[360] GDPR (32) preambulum-bekezdése
[361] GDPR (42) preambulum-bekezdése

összekapcsolt vagy szerződéskötés, szolgáltatás igénybevétele által megkövetelt hozzájárulás megadása.[362] Ilyen esetekben ugyanis az érintett nincs azon helyzetben, hogy szabadon, túlzott külső ráhatás 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.[363]

Ugyancsak nem tekinthető jogszerűnek, ha például egy szupermarket a webáruházában vásárló fogyasztók online viselkedését marketing célból – külön hozzájárulás bekérése hiányában – elemzi, feltételezvén, hogy a vásárlók a webáruházból történő megrendeléssel a marketing célú viselkedéselemzéshez is hozzájárultak.[364] Szintén problémás lehet több célból, illetve több adatkezelő által történő adatkezeléshez adandó hozzájárulások összekapcsolása, ilyen esetben ugyanis az érintett jellemzően nincs abban a helyzetben, hogy külön-külön hozhasson akaratának megfelelő döntést a hozzájárulás megadásáról. A frankfurti felsőbíróság megfelelőnek tartotta azonban a több adatkezelő általi marketing tartalom küldéséhez való hozzájárulást, amelyben gáz- és elektromos szolgáltatásokat jelöltek meg, így az érintett a szolgáltatók pontos listájának előzetes ismerete hiányában is tisztában lehetett vele, hogy milyen szolgáltatásokat bemutató tartalmakat fog kapni.[365]

A fentieken túl a hozzájárulásnak ugyancsak konkrétnak, valamint megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Így a hozzájárulásnak konkrét és meghatározott adatkezelésre szükséges felhatalmazást adnia, valamint abból egyértelműen következnie kell az adatkezelő számára az érintett akaratának, egyben az adatkezelés hozzájárulás által megadott terjedelmének. A hozzájárulásnak mindemellett megfelelő tájékoztatáson kell alapulnia, ennek hiányában ugyanis az érintett nem rendelkezhet kellő tudással az adatkezelés körülményeiről. Ennek kapcsán az Európai Adatvédelmi Testület hozzájárulásról szóló iránymutatása is

[362] GDPR (43) preambulum-bekezdése
[363] Lásd: NAIH/2020/2729/15. 10.
[364] A GDPR (47) preambulum-bekezdésével összhangban azonban nem szükséges azonban 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). Jellemzően azonban a fentiekhez hasonló, korábbi kapcsolat esetén sem számíthat az érintett észszerűen személyes adatainak MI általi, jellemzően viselkedéselemzéssel járó kezelésére, így ilyen esetekben egyéb jogalap hivatkozása szükséges.
[365] OLG Frankfurt am Main, Urteil vom 27.06.2019 - 6 U 6/19, https://openjur.de/u/2185336.html [2023.09.11.]

meghatározást ad a tájékozott hozzájárulás minimumfeltételeiről, ideértve 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.[366] 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 az érintettek számára is elérhető, vonatkozó adatvédelmi tájékoztatójába kell foglalnia.[367]

Kiemelendő továbbá, hogy személyes adatok különleges kategóriáinak kezelése esetén a hozzájárulásnak kifejezettnek kell lennie.[368] 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).[369] 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 vagy gombnyomással). 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 tájékoztatása, 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, megnyomása vagy a robot részére tett és általa érzékelt szóbeli nyilatkozat.

[366] 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.
[367] Necz [353]. 11-12.
[368] GDPR 9. cikk (2) bek. a) pontja
[369] 5/2020 Iránymutatás, 23-24.

Kiemelendő, hogy az érintett jogosult 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. Megemlítendő továbbá, hogy a hozzájárulás visszavonását a hozzájárulás megadásához hasonlóan egyszerű módon kell lehetővé tenni.[370]

A hozzájárulás mellett szintén relatíve gyakran hivatkozott jogalapnak tekinthető az érintettel kötött szerződés teljesítése.[371] 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). Így tehát, amennyiben az érintett például egy applikáción keresztül adja meg hozzájárulását az adatkezeléshez, úgy nem tekinthető megfelelő gyakorlatnak, ha az adatkezelő a hozzájárulás visszavonását szóban közölt nyilatkozathoz köti.

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, például egy adatbázis alapján történő kapcsolatfelvétel útján. 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. 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

[370] GDPR 7. cikk (3) bek.
[371] GDPR 6. cikk (1) b) pontja

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 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 tekinthető, és így az adatkezelés jogalapját is ehhez kell 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.[372]

Természetesen a szerződéses viszonyokhoz kapcsolódó egyes adatkezelések kapcsán egyéb jogalapok megválasztása is felmerülhet, amelyek ezen esetekben helyesebbnek tűnnek, 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,[373] 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 történő, illetve fogyasztókkal kötött szerződések esetén fogyasztóvédelmi jogszabályi 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,[374] azonban e tekintetben értelemszerűen még mind az európai uniós, mind jellemzően a tagállami

[372] Hangsúlyozandó, hogy a munkahelyi adatkezeléssel kapcsolatos egyéb szempontok a tanulmány 4. pont j) ii) pontjában kerülnek ismertetésre.
[373] NAIH-3975-1/2021. sz. ügyben hozott határozat, 9.
[374] GDPR 6. cikk (1) c) pontja

szabályozás kialakulóban van, így napjainkban kifejezetten MI alapú adatkezelést megkövetelő jogszabályi követelményekről még kevésbé beszélhetünk, és inkább azon esetek dominálnak, ahol az MI az érintettek hozzájárulása vagy az adatkezelő jogos érdeke alapján kerül alkalmazásra.

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.[375] Olyan esetekben azonban, ahol valamilyen komplex, az adatkezelés kockázatait felerősítő technológiai megoldás kerül alkalmazásra (ideértve különösen egyes MI alapú megoldásokat), azonban különösen vizsgálandó, hogy szükséges-e specifikus jogszabályi felhatalmazás vagy szabályozási keretrendszer. Például, a járvány elleni védekezésre felhatalmazó törvényi rendelkezés kapcsán kérdésként merülhet fel, hogy ezen általános jogszabályi felhatalmazás alapján egy MI alapú megoldással is vizsgálhatók-e a kontakt adatok, vagy ebben az esetben az adatkezelés már túlmutat a demokratikusan megengedhető kereteken? Elegendő érvként szolgál-e a járvány gyorsabb megfékezésének nagyobb esélye, vagy az érintettek kapcsolatainak, esetleges viselkedésének adott esetben túlzott feltárása, és azokba való túlzott állami behatás figyelembevétele okán a lehetséges körben adatvédelmi szempontból kevésbé aggályos, és az érintettek jogait és szabadságait kevésbé érintő megoldás alkalmazására van szükség? Álláspontunk szerint ezek mind olyan kérdések, amelyek csak esetről-esetre ítélhetők meg, és amelyek területén a megfelelő bírósági és adatvédelmi hatósági gyakorlat kialakulásának különösen hangsúlyos szerepe kell, hogy legyen.

A fentebb írtakra tekintettel, az olyan technológiai megoldásokról, illetve ezekkel végzett adatkezelési műveletekről, amelyek azonban a fentebb írtaknál is nagyobb társadalmi behatással bírnak, valamint az érintett magánéletét és viselkedését még nagyobb mértékben befolyásolják, mindenképpen rendeletnek vagy tagállami szinten törvénynek kell rendelkeznie, hiszen ezen esetekben – legalábbis európai kontextusban – a bíróság, illetve a hatóság nem

[375] GDPR (45) preambulum-bekezdés

veheti át a jogalkotó szerepét. Ilyen megoldásoknak tekinthetők különösen az arcfelismerő rendszerek, amelyek alkalmazására – elvi szinten is – csak kivételes esetben kerülhet sor, megfelelő alkotmányos garanciák mellett, ha a technológia alkalmazásának elmaradása elháríthatatlan károkhoz vezetne (például: egy terrortámadás elkövetőinek azonosítása közterületi kamerafelvételeken).

Ugyancsak kérdéseket vet 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 keretrendszer tükrében 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 jelenlegi eljárási jogszabályi rendelkezések keretén 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, egyes szakértői feladatok támogatásával kapcsolatos rendszerek.[376] 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.[377] Emellett a mechanikusnak és statikusnak tekinthető elemzési, mérlegelési folyamatok, valamint az ezekre történő támaszkodás például az arányos kivételek alkalmazása, vagy épp 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.[378]

Olyan esetekben továbbá, ahol a jogalkotó egy-egy állami döntés meghozatalát az MI-re bízza, már elengedhetetlen a megfelelő jogszabályi keretrendszer kidolgozása, amely – legalábbis

[376] Miskolczi Barna, Szathmáry Zoltán, Büntetőjogi kérdések az információk korában – mesterséges intelligencia, big data, profilozás. Budapest, HVG-Orac Lap- és Könyvkiadó Kft., Budapest, 2018. 190-191.
[377] 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, Routledge, London, 2021. 76-80. 79.
[378] Ron Dolin, Technology Issues in Legal Philosophy. In: Daniel Martin Katz, Ron Dolin, Michael J. Bommarito (eds.), Legal Informatics, Cambridge University Press, Cambridge, New York, 2021. 5-23. 23.

napjaink technológiáját tekintve – magában kell, hogy foglalja az emberi felülvizsgálat lehetőségét is. Vélhetőleg először az egyszerűbb adminisztratív, nemperes eljárások kerülnek majd tömegesen robotizálásra (például: cégbejegyzés, hivatalos dokumentumok másolatának kérése, egyes egyszerűbbnek tekinthető közjegyzői eljárások), ezek esetén ugyanis a jogvita esélye, valamint az MI általi tévedés esélye 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 megfontoltságával döntsön. Nehezen lenne elfogadható ugyanis, hogy egy ember bűnössége kérdésében vagy egy gyermekelhelyezéssel kapcsolatos jogvitában emberi döntéshozók helyett az MI hozzon döntést, hiszen ez az igazságszolgáltatás emberarcúságát kérdőjelezné meg.

Ugyancsak érdekes kérdésnek tekinthető adatvédelmi szempontból, hogy egy-egy szakmai szervezet előírásainak történő megfelelés milyen mértékben fogadható el az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges adatkezelésként. Ez irányadó lehet különösen olyan területeken, ahol erős az ön-, illetve társszabályozás, ideértve például a szakmai kamarákat vagy a gyógyszeripari, egészségügyi szervezetek, illetve a médiatartalom-szolgáltatók szakmai szervezeteit. Az ezen szervezetek előírásainak történő megfelelés jellemzően hivatkozható az abban résztvevő, vagy azok előírásainak egyébként alárendelt adatkezelők által, figyelembevéve, hogy ezen szervezetek sok esetben mélyebb piaci és szakmai ismeretekkel bírnak a saját területükön, mint egy külső hatóság, az általuk megfogalmazott előírások pedig sok esetben az adott terület szakmai etikai alapjait képezik. Ez azonban nem minden esetben tekinthető így, adott esetben pedig akár egy szabályozási keretrendszert kidolgozó, illetve létesítő szakmai szervezet is felelősségre vonható az adott területen kialakuló jogsértő adatkezelési gyakorlat lehetővé tételéért vagy megteremtéséért. Így például az IAB Europe reklámipari szervezet „*Transparency & Consent Framework*” elnevezésű, online marketing célú adatkezeléssel kapcsolatos keretrendszerét[379] a belga adatvédelmi hatóság 2022-ben jogsértőnek találta, a szervezetet pedig 250.000 euró összegű

[379] Lásd: IAB Europe, TCF – Transparency & Consent Framework, https://iabeurope.eu/transparency-consent-framework/ [2023.05.14.]

adatvédelmi bírsággal sújtotta.[380] A döntéssel szemben a szervezet jogorvoslattal élt, amelynek keretében az eljáró bíróság előzetes döntéshozatal iránti kérelemmel fordult az EUB-hez. Az ügy kulcskérdése, hogy az érintettek reklámcélú preferenciáit rögzítő numerikus karakterlánc, az ún. „Transparency and Consent String" (TC-string), személyes adatnak tekinthető-e.[381]

Szintén kevésbé tekinthető napjainkban gyakorinak az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükségessé váló adatkezelés,[382] 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.[383] 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 területe (például: erdők vagy egyéb kies, emberi szemszögből nehezen belátható területek megfigyelése drón segítségével) is szűkebb körű adatkezelést tesz lehetővé. 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). Néhány éve például svájci kutatók fejlesztettek egy drónok kapcsán alkalmazható MI megoldást, amely segítséget nyújt például erdős vagy hegyi területen eltűnt emberek megtalálásában, nagy területek könnyebb átfésülésében.[384]

Leszögezendő azonban, hogy létfontosságú érdeken alapuló adatkezelés vonatkozásában azonban nem kizárólag az érintett, hanem akár más természetes személy létfontosságú érdekeinek védelme is alapul szolgálhat az adatkezelésre.[385] Ezen „másik természetes személy"

[380] A belga adatvédelmi hatóság 2022/21. sz. döntése, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf [2023.05.14.]
[381] C-604/22. sz. ügyben előterjesztett előzetes döntéshozatali kérelem, https://curia.europa.eu/juris/showPdf.jsf?text=&docid=268123&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=1280722 [2023.05.14.]
[382] GDPR 6. cikk (1) d) pontja
[383] 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 [2023.05.06.]
[384] Ryan O'Hare, Drones are being 'taught' to search for missing people: AI software works with quadcopters to explore forests and woods, https://www.dailymail.co.uk/sciencetech/article-3440694/Drones-taught-search-missing-people-AI-software-works-quadcopters-explore-forests-woods.html [2023.09.11.]
[385] GDPR 6. cikk (1) d) pontja

definícióját a GDPR nem határozza meg, így e körben vélhetőleg valamennyi olyan természetes személy szóba jöhet, akinek létfontosságú érdekei védelme adott esetben szükségessé teszi az érintett adatainak kezelését. Egy baleset vagy eltűnés esetén ilyen lehet például egy eszméletlen sérült vagy eltűnt személy érdekében a baleset által érintett más személyek, hozzátartozók vagy az érintettről információval bíró egyéb személyek azonosítása, személyes adataik fentiek érdekében való kezelése.

A fentieken mellett külön kihívást jelenthet az MI közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása kapcsán végzett adatkezelés körében történő alkalmazása.[386] 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,[387] azonban a felhatalmazásnak mindenképp konkrétnak kell lennie, valamint konkrét címzetthez kell szólnia.

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*”.[388] 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 adatkezeléssel kapcsolatos esetleges további adatkezelési cél függvényében dönthető el. Ha

[386] GDPR 6. cikk (1) e) pontja
[387] GDPR (45) preambulum-bekezdés
[388] 28/2014. (IX. 29.) AB határozat [43]

azonban a további adatkezelés az eredetitől elkülönül, úgy további jogalap (például adott esetben az adatkezelő jogos érdeke) hivatkozandó.

Az MI alapú adatkezelések esetén különös jelentősége van továbbá az adatkezelő vagy valamely harmadik fél jogos érdekére történő hivatkozásnak. A jogos érdek – a GDPR 21. cikkében írtakkal összhangban – 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*”.[389] 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.[390]

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.[391] 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.[392]

Kiemelendő azonban, hogy az MI alapú adatkezelés esetén az adatkezelői jogos érdek, valamint annak érintetti érdekekkel való összevetése különös gonddal vizsgálandó, tekintettel az MI alapú adatkezelés sajátosságaira (különösen annak sokszor nehézkes áttekinthetőségére, adatéhségére, átfogó hatásaira és eredményeire, a technológia fejlődésével kapcsolatos bizonytalanságokra). Ennek kapcsán figyelembe veendő továbbá, hogy a legtöbb adatkezelési cél jellemzően MI megoldás alkalmazása nélkül is elérhető, az adatkezelő gazdasági érdekei és üzleti elvárásai pedig jellemzően ritkán írják fel az érintetti érdekeket, különösen az újabb technológiák alkalmazása esetén, amelyek az érintettek magánéletére sokszor nagyobb behatással bírnak. Mindemellett bizonyos területeken az MI alkalmazása különös garanciákat

[389] GDPR 21. cikk (1) bek.
[390] GDPR 13. cikk (1) d), valamint (2) b) pontjai
[391] Lásd: NAIH/2020/1154/9. sz. határozat, 39.
[392] Lásd: NAIH/2019/55/5. 17.

kíván az alkalmazási terület sajátosságaira, valamint egyéb társadalmi, etikai szempontokra tekintettel, ideértve például az arcfelismerő rendszerek vagy az MI egyéb megfigyelési célú 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 cégeladás átvilágításával kapcsolatos dokumentumokat vagy egy peres eljárás nagyszámú dokumentációját áttekinteni.

Kiemelendő, hogy amennyiben marketing célból kerül sor az adatkezelésre, úgy az érintett tiltakozása esetén az adatkezelést haladéktalanul meg kell szüntetni, az érintett ezirányú döntési joga ugyanis az adatkezelő marketing érdekei felett áll.[393] 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 az alább ismertetettek szerinti profilalkotás – révén, illetve alapján intéznek. A technológia, valamint a kapcsolódó társadalmi elvárások változásával azonban elképzelhető, hogy a közeljövőben akár egyes MI alapú megoldások révén végzett marketing célú adatkezelési műveletek is elfogadhatóvá válnak, ideértve például azon eseteket, ahol az érintettek befolyásolásának, illetve a személyes adataikkal való visszaélés kockázata alacsonyabb, és az adatkezelés nagyobb fokú transzparencia mellett történik. Ennek kapcsán azonban az adatkezelőnek megfelelő hatásvizsgálatot kell végeznie, amely az esetleges kockázatok körét, valamint az azok kiküszöbölésére, csökkentésére szolgáló intézkedéseket is meghatározza.[394]

Ahogy az a fentiekből is látható, az adatkezelés alapelveinek betartása, valamint a megfelelő jogalap megválasztása az MI általi adatkezelések esetén is különös jelentőséggel bír.[395] Az MI általi adatkezelés esetén különösen fontosnak tekinthető azonban az adatkezelés

[393] GDPR 21. cikk (1)-(2) bekezdései
[394] Az adatvédelmi hatásvizsgálat kapcsán lásd: a GDPR 35. cikkében, az adatvédelmi hatósággal való előzetes konzultációval kapcsolatban pedig a 36. cikkében írtakat.
[395] Az adatkezelés alapelveinek történő megfelelést és a helyes jogalap megválasztását annak szoros összefüggéseire tekintettel más műveinkben is jellemzően egy fejezetben tárgyaltuk. Lásd: Necz [353]. 100-106, Necz [121]. 142-150.

körülményeinek, és az érintettekre gyakorolt hatás megfelelő felmérése, valamint a technikai szempontok figyelembevétele.

d. Az érintetti jogok gyakorlása

Az érintetti jogok jelentős szerepet játszanak a személyes adatok védelme területén, segítségükkel ugyanis az érintettek alapvető információkat szerezhetnek személyes adataik kezeléséről, valamint döntéseket hozhatnak személyes adataik kezelésével kapcsolatban. Ezen jogok technológiai környezetben különösen jelentős szerepet töltenek 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 érvényesíteni az adatkezelőkkel szemben.

A GDPR – korábbi nemzetközi, valamint európai jogtörténeti előzményekre támaszkodva – széleskörben biztosítja az adatvédelmi jogok gyakorlását az adatkezelés által érintett személyekre 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
- automatizált döntéshozatallal, valamint profilalkotással kapcsolatos egyes speciális jogok.[396]

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 dönthessenek. Mindezen jogok az MI általi, valamint a digitális térben folytatott adatkezelések esetén is kiemelt súllyal bírnak, különös tekintettel az adatok könnyebb és nagyobb fokú felhasználására, valamint az

[396] GDPR 1-22. cikk

adatkezelési műveletek nehezebb átláthatóságára. A fentiekre tekintettel azonban az MI általi, illetve számos esetben a digitális térben folytatott adatkezelések végzőinek kiemelt figyelmet kell fordítaniuk az érintettek tájékoztatására, valamint az érintetti jogok gyakorlásának támogatására.

Az érintettek adatvédelmi jogai kapcsán a tájékoztatáshoz való jog kiemelt szerepet játszik, és egyfajta „esernyő jogként" is funkcionál, ugyanis ez teszi lehetővé az érintettek számára, hogy a személyes adataik kezelését áttekinthessék, és ezt követően megfelelően gyakorolhassák adatvédelmi jogaikat. A tájékoztatáshoz való jog emellett szoros összefüggést mutat az áttekinthetőség alapelvével, ugyanis az adatkezelőktől alapelvi szinten elvárható, hogy a személyes adatok kezelése során főszabályként 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, illetve gyakorolhatósága. 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.[397] 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 a kutatás adott, későbbi fázisában is, illetve azokat egyéb célokra is felhasználják-e az MI segítségével vagy másként.

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 a kevésbé lényegesnek titulált technikai adatokat

[397] GDPR 15. cikk (1)-(2) bekezdései

(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.[398]

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.[399]

Kiemelendő azonban, hogy a másolatkéréshez való jog nem érintheti hátrányosan más személyek jogait és szabadságait.[400] Így tehát az érintettre vonatkozó másolat feleslegesen vagy indokolatlan mértékben, illetve módon nem tartalmazhat más személyekre vonatkozó információt. Tehát például, ha az érintett a rá vonatkozó 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 tartalmaz, 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.[401]

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. Ezek azonban jellemzően nem írják felül az érintett érdekeit és jogszerű elvárásait, illetve nem

[398] Svéd adatvédelmi hatóság [321]
[399] C-487/21. sz. ügyben hozott döntés
[400] GDPR 15. cikk (3)-(4) bekezdései
[401] NAIH/2019/1859. 11.

vezethetnek a másolatkéréshez való jog teljes megtagadásához, kiüresítéséhez. Így például az adatkezelő nem tagadhatja meg az érintett másolat kiadása iránti kérelmének teljesítését általánosságban szellemi tulajdonának védelmére hivatkozással.[402] Tekintettel azonban arra, hogy az érintett másolatkéréshez való joga korlátlanul, valamint az adatkezelő vagy mások érdekeinek teljes figyelmen kívül hagyásával nem gyakorolható, lehetőség van arra, hogy az érintettől az adatkezelő pontosítást kérjen az érintett adatkör kapcsán, vagy a kifejezetten szellemi tulajdonának, üzleti titkának védelmét szükségessé tevő részeket kitakarja. Így például egy információbiztonságért felelős korábbi munkavállaló kérheti a volt munkáltatóját, hogy a munkaviszonya alatt keletkezett egyes adatokat a munkáltató kiadja, azonban ez nem jelentheti azt – különösen hosszabb munkaviszony esetén –, hogy a munkáltató valamennyi munkavállalóra vonatkozó adat kiadására köteles lenne. Így egyrészt kérheti, hogy a munkavállaló pontosítson kérelmén, és az adatkezelő kérelmét csak e körben teljesítse,[403] másrészt megtagadhatja azon adatok kiadását, amelyek kifejezetten a munkáltatóra vonatkoznak (például: a munkáltatónak címzett, de a munkavállalónak is megküldött e-mailek vagy korábbi munkahelyi megbeszélések naptárbejegyzései).[404]

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.[405] Ennek pontos összege kapcsán egységes mértékről, számítási módokról 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 amennyiben az érintett például az adott weboldalról könnyen letöltheti a profiljához kapcsolódó adatait, úgy ennek kapcsán költségek felszámítására jellemzően nincs lehetőség. Az adatkezelő azonban például jogosult lehet költségek felszámítására, ha az érintett papíralapon kezelt dokumentumainak másolatait kéri. Ez esetben például nyomtatási költség felszámítható, a munkaerő költsége azonban vélhetőleg már nem, hiszen az adatkezelő által

[402] Lásd: NAIH-3151-2/2021. sz. határozata. 11.
[403] Lásd: Irish Data Protection Commission ("*Data Protection Commission*"; röviden: „**DPA**") Data Protection in the Workplace: Employer Guidance, April 2023, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Data%20Protection%20in%20the%20Workplace%20Employer%20Guidance%20EN.pdf [2023.05.14.]. 4.
[404] Lásd: Uo.
[405] GDPR 15. cikk (3) bek.

alkalmazott munkaerő (például: egy gazdasági társaság vagy más szervezet esetén) jellemzően rendelkezésre áll, és képes elvégezni a nyomtatással járó vagy hasonló egyszerűbbnek tekinthető feladatokat. Így ennek kapcsán elvi szinten olyan ritkább esetben számolhat el az adatkezelő a munkaerővel kapcsolatos költségeket, ha az érintett kérelme nyomán további, különösen speciális szakértelemmel bíró munkaerő, illetve szakértő bevonása, vagy az adatkezelőtől el nem várható időben történő, rendkívülinek tekinthető munkavégzés vagy rendelkezésre állás szükséges.

Az érintettet továbbá az MI általi adatkezelés esetén is megilleti a helyesbítéshez való jog a pontatlan vagy tévesen kezelt, illetve hiányos személyes adatok esetén. Ennek tükrében a helyesbítéshez való jogba beletartozik a pontatlan személyes adatok mellett a hiányos személyes adatok, például kiegészítő nyilatkozat alapján történő, kiegészítése.[406] Így például, ha az érintett részt vesz egy nyelvi kutatásban, ahol egy adott ország vagy terület különböző régióiból származók által alkalmazott kifejezésmódot és íráskészséget elemzik technológiai megoldások 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 nem jogosult olyan korábbi információk kijavítására, amelyek rögzítésük vagy egyéb kezelésük esetén pontosak voltak, és amelyek megőrzése szükséges (például: egy korábban rögzített kamerafelvétel bizonyítékként történő felhasználása egy érintettel folytatott jogvitában). Az érintettel kapcsolatos elavultnak tekinthető vagy már nem releváns információk (például: keresőprogram segítségével elérhetővé tett, az érintettre vonatkozó korábbi sajtócikkek) eltávolítása kapcsán továbbá inkább az érintett elfeledtetéshez fűződő jogának gyakorlása lehet releváns, illetve e célból alkalmas.

Kiemelendő továbbá, hogy korábbi, akár elavultnak vagy tévesnek tekinthető információk megőrzéséhez is fűződhet egyes esetekben adatkezelői érdek, ez pedig különösen igaz az MI alapú kutatásokra, valamint az MI folyamatos fejlesztésére. Az MI jellemzője ugyanis, hogy korábbi hibákból is tanul, illetve egyes adatok összevetése útján képes következtetések levonására. 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.[407] Ilyen esetekben azonban javasolt lehet a vonatkozó pontatlan információt

[406] GDPR 16. cikk
[407] Lásd: Necz [353]. 102-106.

anonimizálni, vagy ha ez szükséges, bizonyos ideig maszkolás vagy egyéb hasonló eljárás útján pszeudonimizálni.

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

- 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.[408]

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, akár az adatkezelőre irányadó jogi kötelezettségként, akár jogszabályi felhatalmazásként (például: lehetővé téve, hogy meghatározott időtartamig bizonyos dokumentumokat, adatokat az adatkezelő megőrizzen). Jellemzőbbnek tekinthető azonban számos területen, illetve esetben a jogi kötelezettség előírása, különösen ideértve az adózási, számviteli, társadalombiztosítási, munkavédelmi, egyéb foglalkoztatással kapcsolatos, illetve fogyasztóvédelmi jogszabályi rendelkezéseket. Természetesen azonban egyéb sajátos területeken, illetve tevékenységek kapcsán is határozhat úgy a jogalkotó, hogy bizonyos adatok, illetve dokumentáció, vagy akár kamera-, illetve hangfelvételek megőrzését meghatározott időtartamra előírja, jellemzően az adatkezelő ellenőrizhetősége, az illetékes hatóság eljárásának megkönnyítése, 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).

[408] GDPR 17. cikk (1) bek.

Jellemzőnek mondható továbbá, hogy ugyan a jogszabály nem ír elő adatmegőrzést, azonban valamely jog gyakorlásához, illetve követelés érvényesítéséhez elévülési időt rendel. Például a magyar Polgári Törvénykönyvről szóló 2013. évi V. törvény („**Ptk.**”) 6:22. § (1) bekezdése akként rendelkezik, miszerint a polgári jogi követelések főszabályként öt év alatt évülnek el. A Ptk. ezen általános, számos kivételt ismerő szabálya gyakran kerül például Magyarországon figyelembevételére az esetleges érintetti követelésekkel vagy érintettek általi károkozásból származó követelésekkel szembeni védekezés kapcsán történő adatkezelések vonatkozásában. Hasonló elévülési idők más tagállamok jogaiban is megtalálhatók, és hasonló helyzetekben szintén jellemzően figyelembevételre kerülnek.

A fentieken túl olyan eset is felmerülhet, ahol jogszabály nem ír elő adatmegőrzést, 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. Ilyen szempont lehet például egy rendezvényt vagy kiállítást követően a résztvevői adatok néhány napon vagy egy héten keresztüli megőrzése az elveszett tárgyak megtalálásában történő segítségnyújtás vagy egyéb hasonló problémák kezelése kapcsán, tekintettel arra, hogy ilyen jellegű panaszokkal, megkeresésekkel az érintettek jellemzően néhány napon belül jelentkeznek, illetve ezek hasonlóan rövid időn belül megoldhatók, illetve megoldódnak. Természetesen azonban ilyen esetekben is szükségessé válhat eltérő, akár jóval hosszabb adatmegőrzés is (például: bűncselekmény elkövetése vagy kártérítési követelés érvényesítése esetén).

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 a részére nyújtott szolgáltatások személyre szabása kapcsán MI alapú megoldással vizsgálja az érintett preferenciáit, úgy az adatkezelő a fenti adatkezelés végzésének 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 alkalmazás vagy technológia jogszabály-változásra vagy újabb hatósági gyakorlatra tekintettel betiltásra kerül. A fentebb írtak szerint azonban az adatok törlése helyett

sor kerülhet azok anonimizálására, 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 a jellemzően az interneten keresztül történő adatkezelések esetén releváns nyilvánosságra, a GDPR előírja, 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 ezen adatokra mutató linkek vagy az adatok másolatának törlését.[409] Mindez releváns lehet például a fenti példánál maradva, ha az érintett preferenciáit az érintett hozzájárulása alapján kezelő marketingszolgáltató ezen adatokat bizonyos weboldalakon az érintett hozzájárulása alapján megosztja. Az érintett hozzájárulásának visszavonása esetén a 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).

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 célból kerül sor.[410]

[409] GDPR 17. cikk (2) bek.
[410] GDPR 35. cikk (1) bek.

Így amennyiben például egy kontaktszemély felkutatására egy MI megoldás alkalmazásával kerül sor, úgy ennek kapcsán a népegészségügyi érdek az adatkezelés vonatkozásában mindaddig hivatkozható, amíg ezen kontaktszemély azonosítása szükséges. Ugyancsak hivatkozható lehet a jogi igények védelme érdekében szükséges adatkezelés, ha az adatkezelő az érintett egy digitális asszisztenssel folytatott beszélgetését kívánja megőrizni, mindaddig, amíg az érintett reálisan követelést érvényesíthet az adatkezelővel szemben (például egy vitás helyzetben). Hangsúlyozandó azonban, hogy a fenti kivétel-szabályok korlátlanul vagy pusztán általában vett hivatkozásként nem alkalmazhatók. Így tehát például egy arcfelismerő kamerarendszert alkalmazó adatkezelő nem figyelheti folyamatos jelleggel az irodahelyisége teljes területét arra hivatkozással, hogy a technológia alkalmazása, illetve a felvételek egy esetleges betörés esetén az elkövető azonosításához adott esetben szükségesek lehetnek.

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 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.[411]

Az érintett tehát 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 fontos lehet az

[411] GDPR 18. cikk

MI tanulási folyamata, illetve a későbbi hibák elkerülése szempontjából.[412] Így ezen jog gyakorlása jellemzően emberi ügyintéző segítségével foghat helyt (például: ügyféladatok kiigazítása, amelyeket az MI alapul vehet digitális asszisztensi támogatás során), vagy bizonyos egyszerűbb esetekben akár az adott MI megoldás igénybevétele útján, a felhasználási folyamat részeként is támogatható. Így tehát például maga az adott digitális asszisztens alkalmazás intézkedhet az egyszerűen és gyorsan teljesíthető érintetti kérelmek, köztük az adatkezelés korlátozása iránti kérelem 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 rögtön elbírálható, úgy maga is kijavíthatja. Ennek kapcsán azonban hangsúlyozandó, hogy a fentiek kapcsán csak olyan kérelmek elbírálásában vehet részt az MI, amelyeket képes az irányadó jogszabályokkal – így az EU-n belül elsősorban a GDPR-al összhangban – kezelni. Mindaddig, amíg erre az MI bizonyíthatóan nem képes, szükséges emberi ügyintéző bevonása az adott kérelem kapcsán. Az MI azonban ilyen esetekben is képes lehet arra, hogy például az érintett által pontatlannak vagy jogellenesen kezeltnek jelölt adatokat zárolja, és az adott ügyintéző, szakértő vagy szakterület felé továbbítsa az érintett kérelmét, illetve segítsen az érintettel 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 adatkészlettől. Így tehát azokat az adatkezelőnek vagy egyértelműen meg kell jelölnie, vagy külön adathordozóra, illetve erre a célra szolgáló adatbázisba kell helyeznie. Mindennek célja az adatkezelés felfüggesztése az adott adat vonatkozásában annak tisztázásáig, illetve az érintetti kérelem teljesítéséig. Mindez az MI esetén problémákba ütközhet, hiszen míg az MI képes lehet azonosítani a „problémás” adatot, azok „aktív” adatkészletből való eltávolítása számos esetben kérdésesen valósítható meg, hiszen a vonatkozó adatok szükségesek lehetnek az MI működéséhez. Ennek kapcsán a hangsúly inkább az adott adat azonosításán, és ennek kapcsán az érintettre gyakorolt negatív hatások megszüntetésén kell, hogy legyen. Így például, ha a vonatkozó téves információk rögtön korrigálhatók, azokat az MI-nek vagy az azt felügyelő ügyintézőnek mielőbb javítania kell, hogy a továbbiakban téves információk alapján ne legyen folytatható adatkezelés.

[412] Lásd: Necz [353]. 108.

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 további, zárolt kezelésére az érintettnek vagy hatóságoknak történő kiadásig, egy ilyen felvétel segítheti ugyanis annak alátámasztását, hogy az érintett adott időpontban hol tartózkodott, illetve alátámaszthatják adott esetben az érintett téves azonosítását is.

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.[413] 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. Hangsúlyozandó azonban, hogy e tekintetben is lehetnek korlátozások, amely esetekben ezen jog nem gyakorolható, ideértve különösen, amennyiben az adattovábbításnak technikai akadálya merülne fel.[414] Így például, amennyiben az adatkezelő olyan technikai megoldást vagy eljárást alkalmaz, amelynek hasonló alkalmazása a másik potenciális adatkezelőnél nem biztosított, úgy értelemszerűen az adathordozhatósághoz való jog nem gyakorolható. A gyakorlatban ugyancsak problémát jelent e körben, amennyiben a továbbításhoz üzleti titok vagy szellemi tulajdon által védett megoldás felfedésének szükségessége merülhet fel. Ezen esetek egy része tekinthető továbbá technikai akadálynak is (például: forráskód felfedésének vagy új szoftverek beszerzésének szükségessége merülne fel), emellett ezen helyzet jellemzően az érintett személyes adatok védelméhez fűződő jogának, valamint az adatkezelő szellemi alkotások védelméhez fűződő, elsősorban vagyoni érdekének 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 tulajdonjogi érdekei adott esetben erősebbek lehetnek, különösen akkor, ha például kulcsfontosságú szellemi tulajdon felfedése válna szükségessé versenytárs számára, vagy az adattovábbítás megszervezése aránytalan teherrel, indokolatlan

[413] GDPR 20. cikk (1)-(2) bekezdései
[414] GDPR 20. cikk (2) bek.

költségekkel járna. Ezt azonban vita esetén az adatkezelőnek szükséges bizonyítania. Adott esetben akár az érintett kérelme a fenti információk kitakarásával is teljesíthető.[415]

Hangsúlyozandó továbbá, hogy ezen jog csak azon esetekben gyakorolható, amennyiben az adatkezelés az érintett hozzájárulásán vagy a közvetlenül vele kötött szerződésen alapul és az adatkezelés automatizált módon történik.[416] Így tehát, amennyiben az érintett személyesen egy digitális asszisztens vagy chatbot szolgáltatást rendel, úgy ezen jog – elméletileg – gyakorolható, míg ha az érintettet foglalkoztató gazdasági társaság szerződik a szolgáltatóval, és az érintett ezen megállapodás keretein belül használja a digitális asszisztens vagy chatbot alkalmazást, úgy nem. 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.[417]

A fentieken túl megemlítendő, hogy az érintett adathordozhatósághoz való joga nem érintheti hátrányosan mások jogait és szabadságait.[418] Így például 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.

Az érintett tiltakozási joga a közérdekű, illetve közhatalmi jogosítvány gyakorlásának keretébe tartozó, valamint a jogos érdek alapján végzett adatkezelések esetén bír relevanciával, e körbe értve a profilalkotást is.[419] 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.[420] Ezt az adatkezelőnek – a fentebb írtak szerint – az érdekmérlegelési tesztben szükséges levezetnie, az érintetti és az adatkezelői érdekek egyértelmű azonosításával és összemérésével, amelynek összefoglalásaként az adatkezelő vagy harmadik fél jogos érdekeit az adatvédelmi tájékoztatóban is szükséges megjeleníteni.[421]

[415] Necz [353.]. 109-110.
[416] GDPR 20. cikk (1) bek.
[417] GDPR 20. cikk (3) bek.
[418] GDPR 20. cikk (4) bek.
[419] GDPR 21. cikk (1) bek.
[420] Uo.
[421] GDPR 13. cikk (1) d) pontja, 14. cikk (2) b) pontja

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.[422] 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.

Az érintett tiltakozási jogára legalább az első kapcsolatfelvételkor köteles az adatkezelő felhívni az érintett figyelmét, az erre vonatkozó egyértelmű tájékoztatást pedig elkülönítve kell megjeleníteni.[423] Erre sor kerülhet például az adott szöveg kiemelésével, az adatvédelmi tájékoztató kiemelt részén való megjelenítéssel vagy bármely más technikával vagy eljárással, amely az adott esetben az érintett részére megfelelő figyelemfelhívásként értelmezhető.

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.[424] Így amennyiben egy adott hatóság közérdekű feladatai körében gyűjt statisztikai adatokat az érintettről, úgy e körben a tiltakozás értelemszerűen nem foghat helyt.

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.[425] Ilyen esetekben értelemszerűen az MI alkalmazása különösen a fogyasztói akarat manipulálásához, eltorzításához, valamint negatív társadalmi és gazdasági hatásokhoz vezethet. Adott esetben azonban vita tárgyát képezheti, hogy az MI által meghozott döntés joghatással vagy ahhoz hasonló jelentős hatással jár-e az érintettre. Joghatással bírhat például egy

[422] GDPR 21. cikk (2)-(3) bekezdései
[423] GDPR 21. cikk (4) bek.
[424] GDPR 21. cikk (6) bek.
[425] GDPR 22. cikk

szerződéskötés vagy szociális juttatás megtagadásával járó döntés, hasonló jelentős hatással pedig például egy, az érintettek választási szabadságát érdemben befolyásoló, hosszútávú vagy az érintett helyzetére, életére jelentős hatással bíró döntés (például: hitelnyújtással, egészségügyi szolgáltatások igénybevételével kapcsolatos döntés).[426] Így amennyiben például egy bank kölcsönszerződés megkötésére, és az érintett hitelkockázatának ezt megelőző kiszámítására használ egy MI alapú megoldást, és az érintettel való szerződéskötést az MI döntésétől teszi függővé, ez esetben joghatással járó döntésről beszélhetünk, míg amennyiben egy egészségügyi szolgáltató MI alapú megoldás segítségével dönt egy-egy járóbetegnek nyújtott terápia meghosszabbításáról, úgy joghatáshoz hasonló jelentős hatásról beszélhetünk.

Valamennyi esetben azonban csak akkor alkalmazhatók a GDPR automatizált döntéshozatalra, illetve profilalkotásra vonatkozó követelményei, 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 egy-egy szempont kapcsán lát el kisebb jelentőségű számítási vagy adminisztratív feladatokat, úgy automatizált döntéshozatalra ténylegesen nem kerül sor. [427] Hangsúlyozandó azonban, hogy az automatizált döntéshozatal megléte, valamint annak érintettre gyakorolt hatásai jellemzően csak esetről-esetre ítélhetők meg, 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 fog sor kerülni, amely esetben a jelen fejezetben foglalt garanciáknak, szempontoknak is érvényesülnie kell.[428]

[426] 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.
[427] Lásd: Automatizált Döntéshozatallal és Profilalkotással kapcsolatos Iránymutatás, 9.
[428] Lásd: Automatizált Döntéshozatallal és Profilalkotással kapcsolatos Iránymutatás, 22.

Tekintettel arra, hogy az automatizált döntéshozatal, illetve a profilalkotás kiemelt hatásokkal járhat az érintettek jogaira és szabadságaira, 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.[429]

Kiemelendő, hogy amennyiben az automatizált döntéshozatallal, illetve profilalkotással járó adatkezelés a fentebb írtak szerint az érintett 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.[430] Így tehát amennyiben az érintett hozzájárulása alapján nyújt a részére az adatkezelő MI megoldás elemzésével marketing ajánlatokat, úgy az érintett kérheti, hogy ezen ajánlatokat emberi ügyintéző is vizsgálja felül (például: számítási vagy egyéb hiba okán kedvezőtlenebb ajánlat nyújtása esetén), továbbá a döntés (és így jelen esetben az ajánlat, valamint annak meghozatala, alapul fekvő és felhasznált információk) kapcsán észrevételeket tehet, és kifogással élhet az adatkezelőnél az MI által hozott döntéssel kapcsolatban.

A GDPR a fentieken túl rendelkezik az azonosítást nem igénylő adatkezelésről is, amely a digitális világ adatkezelései, illetve az MI általi adatkezelés esetén különösen releváns lehet. 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.[431] Így 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

[429] GDPR 22. cikk (2) bek.
[430] GDPR 22. cikk (3) bek.
[431] GDPR 11. cikk (1) bek.

nem igényli személyes adatok kezelését. Amennyiben azonban az adatkezelő bizonyítani tudja, hogy nem képes az érintett azonosítására, úgy lehetőség szerint köteles őt erről tájékoztatnia. 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.[432]

Kiemelendő továbbá, hogy az érintett kérelmére történő válaszadást, illetve intézkedést díjmentesen kell biztosítani.[433] Amennyiben az érintett kérelme egyértelműen megalapozatlan vagy túlzó (különösen ideértve az ismétlődő kérelmeket), az irányadó adminisztratív költségekre tekintettel az adatkezelő észszerű összegű díjat számíthat fel a kérelem teljesítése kapcsán, vagy megtagadhatja az adatkezelést.[434] A fenti körbe tartozhatnak különösen az indokolatlanul, rövid időn belül ismétlődő, illetve zaklató jellegű megkeresések, ideértve adott esetben az adatkezelő adott munkatársait célzó, zaklató jellegű megkereséseket is.[435] Értelemszerűen ezen szabály azonban az MI általi adatkezelések esetén általában kevésbé hivatkozható, hiszen ez esetben jellemzően automatizált adatkezelésről beszélünk, ahol az ismétlődő kérelmek is sok esetben könnyedén teljesíthetők. Számos közösségi médiaoldal vagy más online platform lehetővé teszi továbbá a felhasználóknak a felhasználói fiókjukkal, adott platformon való aktivitásaikkal, interakcióikkal kapcsolatos adataik letöltését, így könnyítve meg az érintetti kérelmek gyors és hatékony teljesítését.[436]

Az érintetti jogok mellett a jogorvoslati lehetőségek érvényesítéséről is érdemes említést tenni, mivel az érintetti jogok megsértése esetén ténylegesen ez biztosít lehetőséget az érintett jogainak, érdekeinek védelmére. Ennek keretein belül az érintett panaszt tehet az illetékes adatvédelmi felügyeleti hatóságnál,[437] illetve a hatóság döntésével, vagy magával az adatkezelővel, illetve adatfeldolgozóval szemben is bírósági jogorvoslattal élhet.[438] Habár a GDPR általánosságban expressis verbis nem követeli meg az érintettek jogorvoslati lehetőségekről való tájékoztatását, az átlátható adatkezelés, valamint az elszámoltathatóság

[432] GDPR 11. cikk (2) bek.
[433] GDPR 12. cikk (5) bek.
[434] Uo.
[435] Information Commissioner's Office, When can we refuse to comply with a request? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/when-can-we-refuse-to-comply-with-a-request/ [2023.08.25.]
[436] Meta, View and download your Meta account information, https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/view-your-information-and-download-your-information/ [2023.08.25.]
[437] GDPR 77. cikk
[438] GDPR 78-79. cikkek

elvéből következően az adatkezelőtől elvárható, hogy az érintett figyelmét felhívja a jogorvoslati lehetőségekre, az érintetti kérelem teljesítésének elmaradása esetén pedig köteles a panasz, illetve a bírósági jogorvoslat lehetőségéről tájékoztatni az érintettet.[439] Hangsúlyozandó, hogy ahogy az érintetti jogok, úgy a jogorvoslati lehetőségek nem csorbíthatók, korlátozhatók vagy köthetők feltételhez (így például az adatkezelő általános szerződési feltételeiben sem), ez ugyanis az érintettek jogainak és lehetőségeinek aránytalan korlátozásával járna. A tagállami jogok azonban a jogorvoslati lehetőségek gyakorlása, valamint az azokra vonatkozó adatkezelői tájékoztatás megfogalmazása során figyelembe veendők (például: illetékes hatóság, bíróság megjelölése, elérhetőségei).

Hangsúlyozandó továbbá, hogy az érintetteket eltérő jogok illethetik, vagy adatvédelmi jogaik adott esetben eltérően érvényesíthetők a GDPR-tól eltérő, egyéb adatvédelmi jogszabályok hatálya alá tartozó adatkezelések esetén, ideértve például a Bűnügyi Adatvédelmi Irányelv hatálya alá tartozó adatkezeléseket, így a személyes adatok MI általi adatkezelése esetén is elsőként azonosítandó az irányadó adatvédelmi szabályozás, amelyre tekintettel szükséges az adatkezelőnek az érintetti jogok gyakorlását biztosítania, illetve támogatnia.

e. Az adatvédelmi hatásvizsgálat szempontjai

A GDPR alapvető fontosságúként 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 az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába*” (beépített adatvédelem).[440] Mindemellett az adatkezelő „*megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét*

[439] Lásd: GDPR 12. cikk (2) és (4) bek.
[440] GDPR 25. cikk (1) bek.

adatkezelési cél szempontjából szükségesek" (beépített adatvédelem).[441] 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.[442]

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 dokumentált adatvédelmi hatásvizsgálatot végezni, amelyben számot ad az adatkezelésnek az érintett adatvédelmi jogaira gyakorolt hatásairól.[443] Az adatvédelmi hatásvizsgálat részleteit, lefolytatásának lépéseit, valamint annak eredményét, következtetéseit a fentiekre tekintettel egy dokumentáció foglalja össze, amelynek segítségével egyben az adatkezelő az adatkezelés jogszabályi és adatvédelmi hatósági gyakorlatnak való megfelelését is igazolni tudja.

A fentieken túl az adatvédelmi hatásvizsgálat keretében az adatkezelő az adatkezelési művelet körülményeinek és az érintett érdekeinek figyelembevételével olyan intézkedéseket szükséges végrehajtani, amely garantálja az érintett jogainak és érdekeinek védelmét. Így például közlekedési adatok kezelése kapcsán az adatkezelő köteles az érintett által látogatott területek és az érintett útvonalának sajátosságait is figyelembe venni, adott esetben pedig az útvonal kezdetére és végére vonatkozó információkat törölni, annak érdekében, hogy az érintett az általa használt útvonal alapján ne legyen azonosítható.[444]

Az adatvédelmi hatásvizsgálat különös jelentőséggel bírhat az olyan esetekben, ahol bizonyos adatkészleteket az adott MI alkalmazás kiképzéséhez használnak. Így például, amennyiben egy

[441] GDPR 25. cikk (2) bek.
[442] Uo.
[443] GDPR 17. cikk (3) bek.
[444] 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.

biztosítótársaság MI megoldást 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 megoldás kiképzésére, úgy egyrészt fontosnak tekintendő naprakész információk felhasználása (például: korábbi ügyfelekre, megszűnt biztosítási szerződésekhez kapcsolódó információk kezelésének elkerülése), valamint a megoldás és az eredmények megfelelő tesztelése. Mindemellett a megoldás kiképzését és éles alkalmazását követően is fontos az eredmények felülvizsgálata és az algoritmus szükség esetén való módosítása.[445]

f. A mesterséges intelligencia és az adatvédelmi tisztviselő

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.[446]

Az adatvédelmi tisztviselőnek jogi vagy egyéb (például: informatikai) szakképzettséggel nem szükséges rendelkeznie, azonban szakmailag rátermettnek kell lennie, és megfelelő, gyakorlati szintű ismerettel kell rendelkeznie adatvédelmi kérdésekben.[447] Nagyobb szervezeteknél gyakorinak tekinthető, hogy jogi, illetve – különösen technológiai nagyvállalatok esetén – informatikai szakember kerül kijelölésre adatvédelmi tisztviselőnek, még kisebb szervezetek (ideértve például: kis- és középvállalkozások) esetén jelentősnek mondható egy-egy adatvédelmi ügyek kezelésére kijelölt, vonatkozó képzésen részt vett munkatárs vagy külső szakértő (például: megbízási szerződés alapján eljáró ügyvéd) kijelölése. Különösen szervezeten belüli pozíciók esetén azonban kiemelten fontos olyan személy választása, akinek az esetleges további feladatai és kötelezettségei nem ütköznek az adatvédelmi tisztviselői pozícióból fakadó feladatokkal.[448] Így például összeférhetetlenséghez vezethet szervezeten belüli egyéb vezető pozíció (például: vezérigazgató, HR igazgató) betöltése, rövid vagy

[445] 4/2019. sz. Iránymutatás, 26.
[446] GDPR 38. cikk (1) bek., 39. cikk (1) bek.
[447] 37. cikk (5) bek.
[448] GDPR 38. cikk (6) bek.

határozott idejű munkaviszony, alacsonyabb szintű vezetőknek történő közvetlen jelentési kötelezettség.[449] 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.[450]

Adatvédelmi tisztviselővé kijelölhető továbbá akár jogi személy (például: ügyvédi iroda, szakértői szervezet) is, ilyen esetekben azonban az adatvédelmi hatósági gyakorlat jellemzően elvárja olyan természetes személy kijelölését, tulajdonképpeni delegálását a jogi személy részéről, aki az adatvédelmi tisztviselői tevékenységet ténylegesen ellátja, és személyében is megfelel az adatvédelmi tisztviselővel szemben támasztható szakmai tudással kapcsolatos elvárásoknak.

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.[451]

Természetesen adatvédelmi tisztviselő olyan esetekben is kijelölhető, ha az a fentiek szerint nem kötelező. Vállalkozáscsoport[452] emellett közös adatvédelmi tisztviselőt is kijelölhet, ha ez valamennyi tevékenységi helyről könnyen elérhető,[453] így például valamennyi olyan országban, illetve területen képes az adatkezelési folyamatokat felügyelni, illetve a hatósággal és

[449] EDPS, Data Protection Officer (DPO), https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en [2023.08.31.]
[450] Szabó Endre, Az adatvédelmi tisztviselőről. A GDPR szabályainak elemzése, Infokommunikáció és jog, 2018/1. 3-10. 7.
[451] GDPR 37. cikk (1) bek.
[452] GDPR 4. cikk 19. pontja szerint vállalkozáscsoportnak minősül „*az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások.*"
[453] GDPR 37. cikk (2) bek.

érintettekkel való kommunikációba bekapcsolódni, ahol a vállalkozáscsoport tagjai jelen vannak. Erre azonban sor kerülhet helyi szakértők vagy a személyzet erre kijelölt tagjainak támogatásával is.

Természetesen az adatvédelmi tisztviselő működéséhez, valamint tevékenységének sikeres ellátásához az adatkezelő, illetve az adatfeldolgozó köteles megfelelő forrásokat biztosítani.[454] Ezen források körébe tartozhatnak MI alapú vagy egyéb magas szintű technológiai megoldások, figyelembe véve az adatkezelő, illetve adatfeldolgozó, valamint az általa folytatott tevékenységek, adatkezelési műveletek sajátosságait is. Például egy számos, nagy mennyiségű személyes adatot tartalmazó adatbázist üzemeltető adatkezelőnek szükséges lehet olyan informatikai megoldások alkalmazásáról gondoskodnia, amelyek lehetővé teszik az egyes érintettekre vonatkozó információk kiválasztását. Ilyen esetben az adatvédelmi tisztviselőnek vagy az adatkezelő által e célra kijelölt más segítő személynek is szüksége lehet a fenti alkalmazás ismeretére vagy használatára, így az érintetti megkeresések hatékonyan teljesíthetők, az adatvédelmi tisztviselő felügyelete és szükséges körű bevonása mellett.

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.[455] 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? Ha napjainkban még nem is, a közeljövőben ugyanis elképzelhető olyan MI alkalmazás kifejlesztése, amely már képes lesz 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

[454] GDPR 38. cikk (2) bek.
[455] GDPR 38. cikk (3) bek.

emberi ítélőképesség, valamint a szakmai és jogi értelemben vett felelősség hiánya okán kérdőjelezhető meg az MI adatvédelmi tisztviselői tisztség betöltésére való alkalmassága. Hiszen még a jogi személyek, például, jogi – és vezetőiken, munkavállalóikon keresztül – közvetve szakmai értelemben is elszámoltathatók, úgy az MI önmagában nem vonható felelősségre, és nem várható tőle az emberihez vagy akár egy jogi személyhez hasonló tevékenységszervezés sem. Erre tekintettel, ha ilyen MI alapú megoldás kerül alkalmazásra adatvédelmi tisztviselői feladatok ellátására, úgy nem maradhat el az ezen megoldást felügyelő emberi szakértő kijelölése sem. Ha pedig jogi személy kínál ilyen MI alapú megoldást (például: adatvédelmi tisztviselői tevékenység ellátását, szolgáltatás nyújtását igénylő vállalkozások részére), úgy szükséges olyan emberi szakértőt, illetve munkatársat kijelölnie, amely képes az MI alapú alkalmazás tevékenységének, az általa hozott döntések felülvizsgálatára.

Természetesen a fentebb írt MI alapú adatvédelmi tisztviselőknél valószínűbbnek tűnik az adatvédelmi tisztviselőket, valamint a vállalkozások adatvédelmi megfelelését segítő MI alapú megoldások elterjedése, tekintettel arra, hogy ehhez hasonló megoldásokat már számos vállalkozás, illetve egyéb szervezet is alkalmaz. Az ilyen megoldások jelentős segítséget nyújthatnak az adatvédelmi tisztviselők, illetve az egyes adatkezelők és adatfeldolgozók részére, sok esetben időt spórolva meg, valamint megkönnyítve az egyes tevékenységek hatékony összehangolását és ellátását, és a jogszabályi megfelelést.

g. Az adatkezelés ellenőrzése

Az MI általi adatkezelés megfelelő gyakorlatának és környezetének kialakítása szempontjából különös jelentőséggel bírnak az adatvédelmi és egyéb, MI általi adatkezelést felügyelő hatóságok. Ennek tükrében maga az MI Rendelet Tervezet is meghatározza, miszerint a tagállamok kötelesek nemzeti illetékes hatóságot létrehozni vagy kijelölni az MI Rendelet Tervezet alkalmazásának és végrehajtásának biztosítása céljából.[456] Ezen hatóság tehát az MI Rendelet Tervezetnek való megfelelés biztosításáért felel, illetve az ebben meghatározott feladatokat látja el, továbbá, amennyiben az adott tagállamban szervezeti és közigazgatási okok indokolják, úgy akár az egyes feladatok több hatóság között is megoszthatók.[457] Ezen hatóság mellett az adott MI-rendszer alkalmazása és az ennek kapcsán folytatott tevékenység tükrében több, illetve egyéb jogszabályok alapján illetékes hatóság is felügyeletet gyakorolhat, ideértve

[456] MI Rendelet Tervezet 59. cikk (1) bek.
[457] MI Rendelet Tervezet 59. cikk (2) bek.

például a GDPR és a nemzeti adatvédelmi jogszabályok alkalmazásának ellenőrzéséért felelős felügyeleti hatóságokat.[458]

Az MI általi adatkezelés kapcsán az illetékes felügyeleti hatóságok a gyakorlatban számos kihívással szembesülnek, ideértve különösen az adatkezelési műveletek nehéz átláthatóságát, gyakran sokszereplős jellegét, valamint az adatkezelés „nemzetköziségéből", az adattovábbítások intenzitásából eredő problémákat, amelyek sok esetben az illetékes hatóság meghatározását is kihívássá teszik. Ezenfelül további kihívást jelent az egyes szakterületek, iparágak és tevékenységek, valamint az alkalmazás technikai környezetének mélyebb ismerete, amellyel a hatóságok nem feltétlenül rendelkeznek, illetve e tekintetben szakértők bevonására szorulnak. Ezen probléma adott esetben akutabb módon is jelentkezhet az olyan demokratikus társadalmak működése szempontjából jelentős intézmények, mint például a sajtó, illetve a médiaszolgáltatók esetén, ahol az esetleges hatósági felügyelet csak megfelelő demokratikus szempontok szerint érvényesülhet.[459] Emellett azonban az egyes hatóságok gyakran eltérő szempontokat fogalmaznak meg, akár a közös, európai uniós jogszabályok alkalmazásával kapcsolatban is. E körbe tartozhat például az egyes technológiai megoldásokkal szembeni tilalmazó fellépés, amely sokszor egy közös európai válaszlépés kirajzolásához vezet, míg más esetben egyes nemzeti hatóságok különösen fajsúlyos véleményét domborítja ki egy adott témában. Így például a Clearview AI nevű amerikai vállalat arcfelismerő szoftverének alkalmazása kapcsán több európai adatvédelmi hatóság is – szinte egységesen – lépett fel, és szabott ki magas összegű adatvédelmi bírságot, egyben az arcfelismerő technológia kockázatos jellegére is felhívva a figyelmet. Ennek kapcsán a francia adatvédelmi hatóság[460] az olasz[461] vagy a görög adatvédelmi hatósághoz[462] hasonlóan 20 millió euró összegű adatvédelmi bírságot szabott ki az adatkezelővel szemben. Ezen hatóságok tehát annak ellenére döntöttek ugyanazon összegű adatvédelmi bírság kiszabása mellett, hogy az adott országok gazdasága és népessége is eltérőnek tekinthető, ahogy vélhetőleg az adott vállalat piaci jelenléte is az egyes országokban. Ezentúl azonban egyes megoldások kapcsán akár az adatkezelési tevékenység

[458] GDPR 51. cikk (1) bek.
[459] Lásd: David Erdos, European Data Protection Regulation, Journalism, and Traditional Publishers. Balancing on a Tightrope? Oxford University Press, Oxford, 2019, impression: 2. 193.
[460] CNIL, Facial recognition: 20 million euros penalty against CLEARVIEW AI, 2022.10.20, https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai [2023.08.28.]
[461] Garante per la protezione dei dati personali („**GPDP**"), Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362], 2022.03.09, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 [2023.08.28.]
[462] Hellenic Data Protection Authority, Imposition of fine on Clearview AI, Inc, 2022.07.13, https://www.dpa.gr/en/en/enimerwtiko/prakseisArxis/imposition-fine-clearview-ai-inc [2023.08.28.]

megszüntetésére is felszólíthat, vagy annak felfüggesztését is elrendelheti az illetékes hatóság. Így az olasz adatvédelmi hatóság például, szokatlan módon, 2023. tavaszán átmeneti tilalmat rendelt el a ChatGPT olaszországi alkalmazása kapcsán, főként jogsértő adatgyűjtés és a felhasználók életkora ellenőrzésének hiánya miatt,[463] amelyet az adatkezelő általi nagyobb átláthatóság biztosítása, valamint a felhasználók és egyéb nem felhasználó érintettek jogainak nagyobb fokú támogatását követően oldott csak fel.[464]

Ahogy azt a fentiekből is láthatjuk, a ritkábban alkalmazott tilalmazás vagy korlátozás, illetve felfüggesztés helyett az egyéb enyhébbnek tekinthető szankciók (például: figyelmeztetés), valamint a bírságkiszabás tekinthetők a leggyakrabban alkalmazott szankcióknak, amelyek közül ez utóbbi – a jogsértő adatkezelő megnevezésén és a döntés nyilvánosságra hozatalán túl – egyben a leginkább húsbavágó. A bírságok összegét tekintve azonban akár egy-egy tagállamon belül is jelentős eltérések mutatkoznak, sokszor nehezen mérhető fel egy adott felügyeleti hatóság gyakorlatát figyelembe véve, hogy az adott jogsértés esetén várhatóan milyen összegű bírság kiszabását tekintheti indokoltnak. Erre tekintettel bocsátotta ki 2022-ben az EDPB bírságkalkulációval kapcsolatos iránymutatását, amely az adott jogsértés és a vonatkozó körülmények tükrében arányos összegű bírság kiszámítását segíti.[465] A fentieken túl azonban az EU-n belül a gyakorlatban az egyes szankció-típusok között is jelentős eltérések mutatkoznak. Így egyes hatóságok jellemzően kevésbé élnek bírságkiszabással (például ideértve az ír adatvédelmi hatóságot), míg más hatóságok jellemzőbb módon döntenek bírságkiszabás mellett. Mindez azonban arra is késztethet bizonyos nagyvállalatokat, hogy adott esetben az engedékenyebb gyakorlattal bíró adatvédelmi hatóságok szerint döntsenek a joghatóság megválasztásáról.[466] Erre tekintettel a bírságkiszabás tekintetében alkalmazott szempontokon túl javasolt lehet az alkalmazott szankciók körét és alkalmazásuk lehetséges eseteit (például: egyes tipikus „forgatókönyvek” meghatározásával) is nagyobb mértékben összehangolni, így egységesebb szankciós gyakorlat alakulna ki az EU-n belül.

[463] GPDP, Artificial intelligence: stop to ChatGPT by the Italian SA
Personal data is collected unlawfully, no age verification system is in place for children, 2023.03.31, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english [2023.08.28.]
[464] GPDP, ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for european users and non-users, 2023.04.28, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490 [2023.08.28.]
[465] EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 1.0, adopted on 22 May 2022.
[466] Szegedi László, Dornfeld László, Polgár Zoltán, Teleki Bálint, A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – egységes szabályozás, eltérő alkalmazás? Infokommunikáció és jog, 2021/1. 10-16. 15.

Sok esetben az együttműködés más, az adott alkalmazás kapcsán illetékes hatóságokkal is akadályokba ütközhet, valamint az egyes hatóságok hatáskörének pontos azonosítása is kihívásokkal járhat. Az utóbbi években például a versenyhatóságok vagy a fogyasztóvédelmi ügyekben illetékes hatóságok több alkalommal léptek fel jelentős online adatkezelési tevékenységet folytató vállalkozással szemben. Kiemelendő azonban, hogy ezen esetekben az eljáró hatóságok a saját hatáskörükben hoztak döntést (például fogyasztóvédelmi vagy versenyjogi kérdésben), az adatvédelmi hatóság hatáskörének érintése nélkül. Így például Magyarországon a Gazdasági Versenyhivatal („**GVH**”) 2018-ban a Google tájékoztatási gyakorlatát vizsgálta a Google-fiókban elérhető egyes funkciók, valamint az Allo chatkliens adatkezelésével és a chatkliens végpontok közötti titkosításával összefüggésben. Az eljárás során, habár a Google adatkezelési gyakorlatára is figyelemmel volt a hatóság, az egyes Google termékek kommunikációit és a Google adatvédelmi jogszabályi megfelelését a hatóság nem vizsgálta, tekintettel arra, hogy ez az adatvédelmi felügyeleti hatóság hatáskörébe tartozik.[467] Emellett a GVH korábban a Facebook-al szemben is jelentős összegű bírságot szabott ki, tekintettel arra, hogy álláspontja szerint a Facebook oldalán közzétett nyilatkozattal ellentétben (miszerint a Facebook használata ingyenes), a felhasználók az adataikkal fizetnek a szolgáltatás igénybevételéért. A Facebook azonban a döntés bírósági felülvizsgálatát kérte, az ügyben végül a Kúria a Facebook-nak adott igazat, és nem tekintette úgy, hogy a Facebook ezen kijelentése a fogyasztók ügyleti döntésének befolyásolására, megtévesztésére lenne alkalmas.[468]

A fentiekre tekintettel vélhetőleg az MI alkalmazása és az MI általi adatkezelés ellenőrzése kapcsán a közeljövőben is több hatóság lesz érintett és fog eljárni a hatásköre szerinti kérdésekben egy MI „szuperhatóság” helyett, amely valamennyi MI alkalmazás kapcsán hatáskörrel bírna. Ezzel egyidejűleg vélhetőleg jelentősebb hangsúly kerül majd az egyes hatóságok együttműködésére, valamint a hatóságok technológiai kérdésekben való szakértelmének növelésére, illetve a nemzetközi szakértői gárda erősítésére, amely adott esetben más szabályozási környezetek logikáját és meglátásait is kiismeri. Fontosnak tekinthető álláspontunk szerint azonban – különösen az adatvédelmi hatósági gyakorlat esetén – az EU-n belül egységes szankciós gyakorlat kialakítása, amely kiszámíthatóbbá teszi a jogsértésekért járó jellemző szankciókat.

h. Az MI és az adatbiztonság

[467] Gazdasági Versenyhivatal VJ/88/2016. sz. ügyben hozott határozata
[468] Kfv.II.37.243/2021/11.

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*”.[469] E körben továbbá példákat is meghatároz (ideértve például a személyes adatok titkosítását vagy álnevesítését).[470] A fentiek körében kiolvasható továbbá, hogy az adatbiztonság körében a GDPR megfelelő technikai és szervezési intézkedéseket is megkövetel, így az adatkezelő vagy adatfeldolgozó által alkalmazott adatbiztonsági intézkedések körét két csoportra bontja.

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 különböző szabályzatokat, a személyzet részére nyújtott képzést, tréninget. A gyakori szabályzatok közé tartoznak a különböző adatkezelési megoldások által indokolt szabályzatok, például kamerarendszer alkalmazásával kapcsolatos szabályzat,[471] információbiztonsági, illetve iratkezelési szabályzatok, valamint jellemzően egy vállalat vagy vállalatcsoport, vagy hasonló nagyobb szervezet teljes adatkezelési gyakorlatát szabályozó belső adatvédelmi szabályzat. Ugyancsak kiemelendőnek tekintendő az adatvédelmi incidensek,[472] valamint az érintetti kérelmek kezelésével kapcsolatos[473] szabályzatok.

[469] GDPR 32. cikk (1) bek.
[470] Uo.
[471] Lásd például az ír adatvédelmi hatóság gyakorlatából: DPA, 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 [2023.09.03.]. 4.
[472] DPA, 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 [2023.09.03.]. 18.
[473] Lásd például: DPA, Subject Access Requests: A Data Controller’s Guide, https://www.dataprotection.ie/sites/default/files/uploads/2022-

A fentebb írtakkal összhangban ezen belső szabályzatok, valamint az adatkezelőnél irányadó adatkezelési gyakorlat kapcsán szükséges az adatkezelőnek a személyes adatok kezelésében résztvevő munkatársak (ideértve különösen: ügyfélszolgálati, HR vagy marketing osztályok, illetve területek munkatársai) részére megfelelő képzést nyújtani, amelynek szükséges kiterjednie az adatkezelő által végzett adatkezelési műveletek átlátására, az érintetti kérelmek megfelelő kezelésére, valamint a megfelelő adatbiztonságra és az adatvédelmi incidensek lehetséges elkerülésére, illetve kezelésére. A képzést új munkatársak esetén belépéskor, illetve az adatkezelésre irányadó szempontok változásakor (különösen ideértve például az adatkezelési műveletek, szabályzatok, eljárásrend, alkalmazott rendszerek adatbiztonsági intézkedések változását), lehetőség szerint ezen változást megelőzően vagy közvetlenül ezen változást követően szükséges végrehajtani. Ez utóbbi körbe tartozhat például egy esetleges adatvédelmi incidens bekövetkezését és elhárítását követően az alkalmazott adatbiztonsági intézkedések, illetve az irányadó incidenskezelési gyakorlat felülvizsgálata. Ugyancsak szükséges lehet a képzést megismételni, ha arra például munkavállalói igény mutatkozna (például: egy-egy komplex adatkezelési művelet kapcsán szükséges a képzés megismétlése). E körben jelentős segítséget jelenthet oktatási anyag, adott esetben a megszerzett tudást ellenőrző kérdések összeállítása, amely például a belső vállalati rendszeren elérhető a munkatársak számára. Amennyiben az adott szervezet rendelkezik adatvédelmi tisztviselővel, úgy ez szintén jelentős segítséget nyújthat az irányadó oktatási, képzési anyag elkészítésében és felülvizsgálatában, valamint általában az adatkezelői személyzet körében az adatvédelmi tudatosság növelésében.

A fentiek körében szintén a megfelelő szervezési intézkedések körébe tartozik a hozzáférési jogok szabályozása, ideértve például az adott pozíció és munkavállalói, szervezeten belüli jogkörök, szerepek által indokolt adatokhoz és dokumentumokhoz való hozzáférést lehetővé tevő jogosultságok biztosítását, továbbá az illetéktelen hozzáféréssel szembeni védelmi intézkedéseket.

Természetesen napjainkban az MI-vel kapcsolatban hozható különös adatbiztonsági intézkedésekről is beszélhetünk. E körben többféle adatvédelmet erősítő technika (angolul: „*privacy enhancing technologies*”) is meghatározható, amelyek a kezelt adatok körének minimalizálása mellett az adatbiztonság szintjét jelentősen megemelik, illetve az érintettek

10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf [2023.09.03.]. 10.

jogainak érvényesítését is biztosítják.[474] E körbe tartozik például a federatív tanulás (angolul: „*federated learning*"), amely lehetővé teszi az MI modellek kiképzése során a tréningadatok külön kezelését, így a modellek kiképzését végző személyek vagy szervezetek anélkül is egyesíthetik tanulási modelljeiket, hogy a kiképzéshez szükséges adatokat megosztanák.[475] Szintén megoldást jelenthet például a homomorfikus titkosítás (angolul: „*homomorphic encryption*"), amely révén számítások végezhetők titkosított adatokon a titkosítás feloldása nélkül is.[476]

Hangsúlyozandó azonban, hogy ezen technikák jellemzően nem biztosítanak önmagukban teljeskörű védelmét. Így például federatív tanulás alkalmazása esetén, az egyes modellek megvizsgálása, visszafejtése révén – közvetett módon – azonosíthatók az érintettek, illetve adataik, így szükséges a federatív tanulást egyéb adatvédelmet erősítő technikákkal kiegészíteni, mint például homomorfikus titkosítással vagy például biztonságos kommunikációs protokollok (angolul: „*secure communications protocols*") segítségével.[477] 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 alacsonyabb szintű adatbiztonsági intézkedések lehetnek szükségesek – adatvédelmi szempontból – egy jellemzően nem személyes adatok kezelésére szolgáló MI megoldás fejlesztése, mint egy nagy számú egészségügyi és egyéb szenzitívnek mondható adat kezelésére alkalmazott megoldás esetén. Hangsúlyozandó azonban, hogy az adatvédelmi szempontokon túl egyéb szempontok is irányadók lehetnek (például: szellemi tulajdon, üzleti titok védelme), továbbá az adott terület, tevékenység kapcsán irányadó különös szabályok, hatósági vagy szakmai gyakorlat is irányadó lehet (például: biztosítótársaságok általi adatkezelés esetén az irányadó adatvédelmi és egyéb jogszabályi rendelkezések, felügyeleti hatóság előírásai iránymutatásai).

Az adatbiztonság kérdéskörén túl az adatvédelmi incidensek kezelése szintén kulcsfontosságúnak tekintendő, az MI általi adatkezelés tekintetében is. Informatikai

[474] 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 [2023.09.03.] ("**ICO PETs Iránymutatás**") 3.
[475] ICO PETs Iránymutatás, 23.
[476] ICO PETs Iránymutatás, 12.
[477] ICO PETs Iránymutatás, 25-26.

környezetben az incidensek alatt számos, az adott rendszert vagy érintett információkat negatívan érintő esemény érthető. Ezzel szemben azonban az adatvédelmi incidensek körét szűkebben, illetve bizonyos szempontból eltérően határozhatjuk meg. Így ezen kifejezés alatt jellemzően olyan incidenst értünk, amely akár technikai, akár más környezetben, de a személyes adatok elvesztéséhez, megsemmisüléséhez, vagy azok egyéb nem kívánt megváltoztatásához, az azokkal való visszaéléshez vezethet. A GDPR is akként határozza meg az adatvédelmi incidenst 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*”.[478]

A fentebb írtakkal összhangban az adatkezelőnek megfelelő incidenskezelési szabályzatot szükséges alkotnia, amely különösen kiterjed az adatvédelmi incidensek kezelésére. Ennek részét képezi az adatvédelmi incidens egyéb incidensektől való elhatárolása is. Előfordulhatnak ugyanis olyan események, amelyek személyes adatokat nem érintenek, és így adatvédelmi incidensnek sem tekinthetők, azonban egyéb jogszabályok követelményeket határozhatnak meg a kezelésükre vonatkozóan, ideértve adott esetben a hálózati és információs rendszerek biztonságával kapcsolatos európai szabályozás tükrében az ún. „*biztonsági eseményeket*”,[479] illetve „*eseményeket*”.[480] Emellett az egyéb szabályozott szakmák és tevékenységek esetén is irányadók lehetnek külön incidens-bejelentési és kezelési szabályok (például: hírközlési szolgáltatókat, bankokat és pénzügyi szolgáltatókat érintő incidensek), illetve hasonló követelményeket támaszthat a specifikus MI szabályozás is. Így az MI Rendelet Tervezet is meghatároz például a nagy kockázatú MI-rendszerek működésével kapcsolatos egyes események automatikus rögzítésére („naplózására”),[481] illetve a súlyos váratlan események és

[478] GDPR 4. cikk 12. pontja

[479] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, OJ L 194, 19.7.2016, p. 1–30 (BG, ES, CS, DA, DE, ET, EL, EN, FR, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV) („**NIS Irányelv**”), 4. cikk 7. pontja értelmében Biztonsági esemény: „*minden olyan esemény, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára*“.

[480] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg), PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80–152 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV) („**NIS2 Irányelv**”), 6. Cikk 6. pontja értelmében esemény : „*olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát*”.

[481] MI Rendelet Tervezet 12. cikk

működési hibák bejelentésére[482] vonatkozó szabályokat. Ennek tükrében a nagy kockázatú MI-rendszerek szolgáltatói az ilyen rendszerek minden olyan súlyos váratlan eseményét vagy működési hibáját kötelesek jelenteni, amely az alapvető jogok védelmét célzó uniós jogi kötelezettségek megszegésével jár, azonban tagállamok piacfelügyeleti hatóságainak, ahol az ilyen esemény vagy jogsértés történt.[483] Az ilyen eseményről vagy hibáról szóló értesítést haladéktalanul meg kell tenni azt követően, hogy a szolgáltató megállapította az MI-rendszer és a hiba vagy esemény közti ok-okozati összefüggést, de legkésőbb 15 napon belül azt követően, hogy a szolgáltató ilyen eseményről vagy hibáról tudomást szerzett.[484] Az MI Rendelet Tervezet EP Változata ennek kapcsán már jóval rövidebb, 72 órán belüli értesítési kötelezettséget ír elő.[485] Amennyiben a fenti hiba egyben adatvédelmi incidensnek vagy egyéb jogszabály szerinti biztonsági 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).

Amennyiben adatvédelmi incidensről van szó, úgy kiemelten fontos 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.[486]

[482] MI Rendelet Tervezet 62. cikk
[483] MI Rendelet Tervezet 62. cikk (1) bek.
[484] Uo.
[485] MI Rendelet Tervezet EP Változata 62. cikk (1) bek.
[486] 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 [2023.09.03.], 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 [2023.09.03.] („**Iránymutatás az Adatvédelmi Incidensek bejelentéséről**”), 8.

Amennyiben az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, úgy szükséges azt bejelenteni az adatvédelmi felügyeleti hatóságnak,[487] amennyiben pedig ezen kockázat valószínűsíthetően magasnak tekinthető, úgy erről az érintettet is késedelem nélkül tájékoztatni kell.[488] 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.[489]

A gyakorlatban esetről-esetre vizsgálandó, hogy a valószínűsíthető kockázat fennáll-e, amely tekintetében az alkalmazott adatbiztonsági intézkedések köre kiemelt jelentőséggel bír. Így a valószínűsíthető kockázat akár nagyobb számú vagy szenzitívebbnek tekinthető 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.[490]

Így tehát, amennyiben az adott MI megoldás kiképzéséhez 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 az érintetteket sem tájékoztatni.

i. A mesterséges intelligencia általi adatkezelés határon átnyúló jellege

A határon átnyúló, illetve az EU-n kívüli, harmadik országokban történő, vagy nemzetközi szervezetek általi adatkezelések sok esetben kiemelt kockázatokat jelenthetnek az érintettek

[487] GDPR 33. cikk (1) bek.
[488] GDPR 34. cikk (1) bek.
[489] GDPR 33. cikk (1), (5) bekezdései
[490] Iránymutatás az Adatvédelmi Incidensek bejelentéséről, 34.

számára, tekintettel az ezen országokban irányadó eltérő, sok esetben enyhébb vagy hiányosnak tekinthető adatvédelmi szabályozásra, valamint a személyes adatokhoz való aktívabb hozzáférésre, illetve a magánszférába való erősebb behatásra az adott országban eljáró hatóságok által. Bizonyos esetekben különös kockázatot jelenthet az érintettre nézve, amennyiben a nyugati demokráciáktól eltérő államszervezettel bíró harmadik országba történik adattovábbítás, tekintettel arra, hogy itt még kevesebb jogszabályi korlátja lehet az érintett adataihoz való hatósági hozzáférésnek, valamint az érintett is szűkebb körű jogérvényesítési lehetőséggel, illetve jogorvoslati eszközzel bírhat a személyes adatainak kezelésével kapcsolatban.

Kiemelendő, hogy az Európai Bizottság megfelelőségi határozatában meghatározhat olyan harmadik országokat, ahol az ide továbbított személyes adatok biztonsága megfelelő védelmi szintet élvez.[491] Ilyen országnak tekinthető például Japán, a Koreai Köztársaság, Svájc, az Egyesült Királyság vagy – az EU-USA adatvédelmi keretrendszerhez (angolul: „*EU-US Data Privacy Framework*”) csatlakozott szervezetek tekintetében – az Amerikai Egyesült Államok.[492]

Az Egyesült Államokba történő adattovábbítás kapcsán az új keretrendszer azért is bír kiemelt jelentőséggel, mivel az EUB korábbi döntéseiben mind az Egyesült Államokba történő adattovábbításhoz alapul szolgáló „biztonságos kikötő” adatvédelmi elvek,[493] mind az ún. adatvédelmi pajzs[494] szerinti adattovábbítást nem tekintette megfelelőnek. Az új keretrendszer azonban remélhetőleg az adattovábbítással kapcsolatban kellő garanciákat biztosít majd ahhoz, hogy kiállja egy esetleges újabb jogvita próbáját.

Amennyiben a fentiek szerinti megfelelőségi határozat nem áll rendelkezésre, úgy a fenti kockázatokra tekintettel a GDPR az illetékes adatvédelmi felügyeleti hatóság engedélyéhez vagy megfelelő garanciák meglétéhez köti a harmadik országokba vagy nemzetközi szervezetek részére történő adattovábbítást, ideértve az alábbiakat[495]:

[491] GDPR 45. cikk
[492] A megfelelő adatvédelmi szintet biztosító országok listájához lásd: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [2023.09.03.]
[493] C-362/14. sz. ügyben hozott ún. Schrems I. ítélet
[494] C-311/18. sz. ügyben hozott ún. Schrems II. ítélet
[495] GDPR 46. cikk (2) bek.

- közhatalmi, illetve egyéb közfeladatot ellátó szervek közötti, jogilag kikényszeríthető erejű eszköz;
- kötelező erejű vállalati szabályok;
- az Európai Bizottság által vizsgálóbizottsági eljárásnak megfelelően jóváhagyott általános adatvédelmi kikötések;
- az illetékes adatvédelmi felügyeleti hatóság által vizsgálóbizottsági eljárásnak megfelelően jóváhagyott általános adatvédelmi kikötések;
- jóváhagyott magatartási kódex;
- jóváhagyott tanúsítási mechanizmus.

A fentebb írtakon túl az illetékes adatvédelmi felügyeleti hatóság engedélye mellett megfelelő garanciaként szolgálhatnak az adattovábbító, illetve az adattovábbítás címzettjének tekinthető adatkezelő, illetve adatfeldolgozó között létrejött szerződéses rendelkezések, valamint közhatalmi, illetve egyéb közfeladatot ellátó szervek közötti megállapodásokkal kapcsolatos egyes rendelkezések.[496] Szintén megfelelő garanciát biztosítanak az illetékes adatvédelmi felügyeleti hatóság által jóváhagyott kötelező erejű vállalati szabályok,[497] amelyek főként multinacionális vállalatcsoportokon belüli adattovábbítások kapcsán bírnak jelentőséggel. Ennek előnye, hogy az adott vállalkozáscsoport saját maga határoz a szabályokról, amely egyben a szabálykövetési hajlandóságot is növelheti, azonban adott esetben a szabályok kijátszására, vagy túlságosan enyhe követelmények támasztására is lehetőséget biztosíthat.[498]

Emellett – az uniós jog által nem engedélyezett adattovábbítás, illetve közlés vonatkozásában – az Unió vagy az érintett tagállam és harmadik ország között létrejött, hatályos nemzetközi megállapodás (például: kölcsönös jogsegélyszerződés) alapul szolgálhat harmadik ország bírósági ítélete, illetve közigazgatási hatósági döntése szerinti adattovábbításhoz.[499] Ennek hiányában azonban, ha más garancia nem áll fenn, úgy önmagában a harmadik országbeli bírósági döntés vagy közigazgatási határozat nem szolgáltat kellő alapot az EU-n belül személyes adatok továbbítására.

[496] GDPR 46. cikk (3) bek.
[497] GDPR 47. cikk
[498] Kis Kelemen Bence, Hohman Balázs, A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra, Infokommunikáció és jog, 2016/2. 64-70. 65.
[499] GDPR 48. cikk

A fentiek mellett a GDPR lehetővé teszi a fenti garanciák hiányában is személyes adatok továbbítását harmadik országba vagy nemzetközi szervezet részére ún. különös helyzetek esetén, ideértve azon eseteket, amennyiben az adattovábbítás

- az érintett kifejezett és tájékozott hozzájárulása alapján történik,
- az érintettel kötött szerződés teljesítéséhez vagy a szerződéskötést megelőző lépések megtételéhez szükséges,
- más természetes személlyel kötött, az érintett érdekeit szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges,
- fontos közérdekből szükséges,
- jogi igények előterjesztéséhez, védelméhez, illetve érvényesítéséhez szükséges,
- az érintett vagy más személy létfontosságú érdekeinek védelméhez szükséges, és az érintett képtelen hozzájárulást adni (például mert eltűnt vagy eszméletét vesztette),
- olyan nyilvántartásból származó adatok vonatkozásában történik, amely az irányadó uniós vagy tagállami jog tükrében a nyilvánosság tájékoztatását szolgálja.[500]

Hangsúlyozandó azonban, hogy az adattovábbításra a fentiek szerinti különös helyzetekben biztosított eltérések esetén csak akkor kerülhet sor, ha az nem ismétlődő jellegű (például: egyszeri, vagy arra csak néhány alkalommal kerül sor), csak korlátozott számú érintettre vonatkozik (így például csak az adatkezelővel szerződést létesítő vagy egyéb módon kapcsolatban álló, illetve kisebb számú, konkrétan meghatározható érintettre), illetve az adatkezelő kényszerítő erejű jogos érdekéből szükséges, amelyet nem írnak felül az érintett érdekei.[501] A fentiekre tekintettel tehát az adatkezelő nem hivatkozhat a fentiek szerinti valamely különös helyzetekben biztosított eltérésre, amennyiben az adattovábbításra rendszeresen vagy nagy számú érintett vonatkozásában kerül sor (ideértve például: harmadik országbeli szolgáltató által chatbot szolgáltatás nyújtását számos EU-n belüli felhasználó részére). Ugyancsak nem kerülhet sor az adattovábbításra, és nem tekinthető különös helyzetben biztosított eltérésnek, amennyiben az adatkezelő MI-alapú megoldás segítségével az érintettek tudta nélkül készít róluk felhasználói profilt szolgáltatásainak személyre szabása, és így még nagyobb profit elérése érdekében. Különös helyzetben biztosított eltérésnek tekinthető azonban amennyiben az érintett egy erdei túra során eltűnt, és a hatóságok csak egy harmadik országbeli MI-alapú megoldást nyújtó szolgáltató segítségével képesek azonosítani;

[500] GDPR 49. cikk (1) bek.
[501] Uo.

ilyen esetekben ugyanis az érintett létfontosságú érdekéről beszélhetünk, amely esetben az érintett nincs abban a helyzetben, hogy az adatkezeléshez hozzájárulását adja, annak elmaradása azonban az érintett életét vagy biztonságát jelentős veszélynek teheti ki.[502]

Mint a fentiek alapján is látjuk, az MI alapú adatkezelés sok esetben határon átnyúló adatkezelést, illetve adattovábbítások láncolatát feltételezi, számos esetben pedig sokszereplős folyamatot vagy folyamatokat feltételez. Gyakori például, hogy egy vállalkozás vagy a hatóságok harmadik országbeli szolgáltatók szakértelmét és szolgáltatásait veszik igénybe, amely esetek egy részében az adattárolás sem az EU-n belül történik, vagy bizonyos esetekben szükségesnek tekinthető a személyes adatokhoz harmadik országból történő hozzáférés (például: eseti jellegű technikai segítségnyújtás szükségessége vagy harmadik országbeli szakértő bevonása). Előfordulhat továbbá, hogy több szolgáltató közösen nyújt MI-alapú szolgáltatásokat, esetleg több eltérő megoldást is alkalmaznak a szolgáltatásaik fejlesztése és nyújtása során, amelyek szolgáltatói bizonyos esetekben vagy szempontok szerint szintén hozzáférnek a személyes adatokhoz. Az ilyen komplexnek tekinthető, többszereplős adatkezelési műveletek jellemzően beható vizsgálatot követelnek meg az abban résztvevő adatkezelők és adatfeldolgozók körének meghatározása, valamint az egyes adattovábbítások és azok egyéb szempontjainak feltérképezése és értelmezése kapcsán. Ennek alapján dönthető el tehát, hogy a személyes adatok továbbítására lehetőség van-e, és ha igen, úgy az milyen garanciák fennálltát, illetve milyen adattovábbítással kapcsolatos további követelményeknek való megfelelést feltételez (ideértve például megfelelő kiegészítő intézkedések meghozatalát)[503].

j. A szektorális adatkezelés kihívásai

Az MI általi adatkezeléssel kapcsolatos főbb kihívások általános megközelítést és szabályozást követelnek meg. Ide tartoznak például az adatkezelés átláthatóságával, az adattovábbítások megfelelőségével, valamint az érintetti jogok biztosításával kapcsolatos kihívások, amelyek az MI általi adatkezelés kapcsán számos esetben, illetve iparágban vagy tevékenységi kör kapcsán jelentősnek mondhatók. Emellett azonban bizonyos esetekben az MI általi adatkezeléssel

[502] GDPR 49. cikk (1) f) pontja
[503] A kiegészítő intézkedések meghozatalával kapcsolatos elemzéshez lásd: EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021. 3-5.

kapcsolatos szektorális szempontok figyelembevétele különösen jelentősnek mondható, az adott szakterület jellemzői pedig az MI általi adatkezelés sokszor különös szempontok szerinti értékelését követeli 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 saját megközelítést követelő esetkörök 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 különösen jelentős társadalomformáló hatásokkal bírhat, az adatvédelmi követelmények helyes alkalmazása ezeken területeken pedig kiemelt jelentőséggel bír, az MI alkalmazásának etikai szempontjai pedig az adatvédelmi szempontokkal szoros összhangban állnak.[504]

i. A mesterséges intelligencia szerepe az egészségügyben

Az MI szerepe, habár napjainkban számos területen mondható jelentősnek, az egészségügy területe 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 azonosításában, illetve klinikai vizsgálatok, kutatások támogatásában.[505] Megemlítendő azonban, hogy az egyes betegségek azonosítása számos esetben kihívást jelenthet a technológia jelenlegi lépcsőfokán, tekintettel arra, hogy a betegségek azonosításához szolgáló megoldások túlérzékenysége vagy túlzott precizitása egyik oldalon számos téves diagnózishoz vezethet, és így a betegeket felesleges orvosi vizsgálatoknak teheti ki, míg a másik oldalon a betegség számos esetben azonosítatlan maradhat, így veszélyeztetve az érintett betegek életét és egészségét.[506] Erre tekintettel értelemszerűen a fenti egészségügyi MI-rendszerek

[504] Kiemelendő, hogy bár a digitalizáció és az adatvédelem szempontjából releváns számos új jelenséget is jelentősnek tekintünk az MI általi adatkezelés kapcsán, azonban a digitalizáció és az adatvédelem egyes közeljövőbeli kihívásaival az alábbiakban külön fejezetben foglalkozunk.
[505] Davenport T, Kalakota R. The potential for artificial intelligence in healthcare. Future Healthc J. 2019 Jun;6(2):94-98. doi: 10.7861/futurehosp.6-2-94. PMID: 31363513; PMCID: PMC6616181. 94.
[506] Hannah Fry, Emberek és gépek. Hogyan tartsuk a kezünkben az irányítást a mesterséges intelligencia korában? HVG Kiadó Zrt, Budapest, 2021. Fordította: Dembinszky Zsófia (2020), eredeti kiadás: 2018. 101.

felülvizsgálata jellemzően nagyobb figyelmet követel meg az üzemeltetők 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 egészségügyi személyzet munkavégzését is. A közeljövőben várhatóan további kihívásokat jelentenek továbbá 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.[507] Maguk a kiborbok és a fentiekhez hasonló ember-gép kapcsolatokra épülő rendszerek bizonyos szempontból el is halványítják a robot és ember közti határvonalat, azonban nem szüntetik azt meg, és ezen rendszerek vagy az azok által érintett emberek sem tekinthetők értelemszerűen robotnak.[508]

Az MI egészségügyi alkalmazása esetén azonban az etikai elvárásoknak való megfelelés kiemelten fontosnak mondható. Ez az MI-vel kapcsolatos általános etikai elvárásokon túl azonban az orvosi és egészségügyi szempontok figyelembevételét is megköveteli. Az egyik legismertebb amerikai orvosi szervezet (American Medical Association, „**AMA**") már évek óta jelentősebb figyelmet szentel az MI egészségügyi és kutatási célú felhasználásának. Ennek kapcsán például „*Augmented Intelligence and Healthcare*" elnevezésű szabályzatában („**AMA Policy**")[509] 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.[510] 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

[507] Klein Tamás, Robotok a beteggondozásban és a gyógyításban. In: Klein Tamás, Tóth András (szerk.): Technológia jog – Robotjog – Cyberjog, Wolters Kluwer Hungary, Budapest, 2018. 210-211. 211.
[508] Udvary Sándor, Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései, Gazdaság és jog 2018/12. 14-21. 15.
[509] AMA, Augmented intelligence in healthcare, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf [2023.09.01.]
[510] AMA Policy, Foundational policy Annual 2018. 1.

felhasználással kapcsolatos bizonyítékok rendelkezésre állását, az automatizáció fokát, az átláthatóságot, valamint az alkalmazás feltételeit.[511]

Emellett kiemelendők az AMA egészségügyi MI megoldások alkalmazásával kapcsolatos felelősségre vonatkozó meglátásai. Így az AMA az adott megoldás megtervezése 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 része lesz majd az orvosi képzésnek és a gyakorlati időszaknak az egészségügyi MI rendszerek alkalmazásának, felügyeletének megfelelő elsajátítása, valamint az azzal való együttműködés.[512]

Az MI egészségügyi alkalmazása kapcsán az érintettek tájékoztatása különösen fontosnak tekinthető, ugyanis az adatkezelés sok esetben sérülékeny érintetti csoportokat (például: betegek, idősek, gyermekek, fogyatékos személyek) érint, akik adott esetben kevésbé képesek átlátni személyes adataik kezelését. Emellett ezen adatkezelési műveletek jellemzően kifejezetten összetettnek mondhatók, amelyek tovább növelik az adatkezelés átláthatóságával kapcsolatos kihívásokat. Így az adatkezelőnek különös gondot kell fordítania az érintettek által értett megfelelő adatvédelmi tájékoztató elkészítésére és közzétételére, illetve az adatkezelés átlátható folytatására, szükség esetén az érintett részére való bővebb vagy ismételt magyarázat adására és az érintetti joggyakorlás támogatására. A fentiek természetesen bizonyos mértékben a betegek egészségügyi jogszabályi, illetve szakmai szabályok szerinti egyéb tájékoztatására is igazak lehetnek, ennek kapcsán a megfelelő mértékű átláthatóság és a betegek egészségügyi, jogi és érzelmi támogatása még nagyobb súllyal bírhat. Kiemelendő azonban, hogy az MI technológiai sajátosságai okán, akár egészségügyi szolgáltatás, akár kutatási célú adatkezelés esetén előre nem jósolható meg sem az MI által hozott valamennyi lehetséges döntés, sem az adatok valamennyi lehetséges jövőbeli felhasználása.[513] Így amennyiben egy radiológiai

[511] AMA Policy, Regulation, payment, liability and other key policies Annual 2019. 2.
[512] 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 [2023.09.01.]
[513] Forti, Mirko, The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR (June 27, 2021). European Journal of Legal Studies 13 (1), June 2021, 29-44, Available at SSRN: https://ssrn.com/abstract=3866576. 35.

felvétel elemzése alapján az MI arra a meglátásra jut, hogy az érintettnél rákos megbetegedés diagnosztizálható, az orvos, vagy a fenti egyéb szolgáltató vagy informatikai szakértő sem lehet feltétlenül képes arra, hogy pontos magyarázatot adjon az MI fenti következtetésére.[514] Ettől függetlenül azonban a megfelelő további vizsgálatokkal és orvosi szakvéleménnyel az MI által levont következtetés 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 a megoldás folyamatos felülvizsgálatával és ellenőrzésével kellő szintű átláthatóságot biztosíthat az adott MI megoldás egészségügyi alkalmazása kapcsán.

Az MI 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 az ún. dinamikus hozzájárulást, amely értelmében a betegek egy interfészen vagy más hasonló felületen keresztül aktív módon kommunikálhatnak az egészségügyi vagy kutatói személyzettel.[515] 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.[516] Mindezen hozzájárulással kapcsolatos megközelítések álláspontunk szerint elgondolkodtató alternatívát javasolnak a lineáris folyamatként tekintett, „klasszikus értelemben vett" hozzájárulás kezelésre, 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 értelmezett dinamikus értelmezése így adott esetben még szélesebb jogérvényesítést biztosít a beteg vagy a nevében eljáró képviselője számára adatvédelmi jogainak érvényesítése érdekében, és a változó, sokszor technikai környezetben történő

[514] Davenport [505]. 97.
[515] Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, Karen Melham, Dynamic consent: a patient interface for twenty-first century research networks, 23 European Journal of Human Genetics, 2015. https://doi.org/10.1038/ejhg.2014.71. 141-146, 141.
[516] 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, 37 MedR, 2019. https://doi.org/10.1007/s00350-019-5247-2. 431-439. 432.

jogérvényesítést is megkönnyítheti, például: egy kórházi robot vagy szoftver által lejátszott hangfelvétel, vagy az adatkezelés újabb szakaszairól küldött emlékeztető útján.[517]

Természetesen a fentieken túl a megfelelő adatbiztonsági intézkedések alkalmazása sem hanyagolható el, ezek révén ugyanis hatékonyabban védhetők az MI által felhasznált személyes adatok, illetve az érintettek. Így, különösen a nagy számú betegadatot MI megoldás útján 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 számos egyéb terület mellett a munkahelyeket és a munkához való viszonyunkat is forradalmasítja. Segítségével ugyanis számos, rendkívül időigényes vagy monoton feladat könnyebben elvégezhető, emellett azonban számos, korábban emberek által betöltött pozíciót is feleslegessé tesz. Ezek napjainkban akár komplexebb feladatok elvégzését megkívánó munkakörök is lehetnek, 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),[518] miközben, jellemzően a technológiai területen eljáró tanácsadók (például: ügyvédek) esetén az MI fejlődése egyre gyorsuló ütemben követeli meg a szakmai tudás naprakészen tartását.[519] Emellett továbbá általánosságban is elmondható, hogy nem kizárólag a munkaerő kiváltását, helyettesítését vonja maga után az MI fejlődése, hanem bizonyos körben a kognitív képességek kialakítását is szükségtelenné, nélkülözhetővé teheti, amelyek szükségesek a megfelelő alkalmazkodóképesség és intelligencia kialakításához.[520] Így a társadalom egyre nagyobb

[517] Eduard Fosch-Villaronga, Robots, Healthcare, and the Law. Regulating Automation in Personal Care, e-book version, 2020. 181-182.
[518] 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 [2023.08.25.]
[519] Deepa Ravindranath, A Guide to Commercial Innovation in Artificial Intelligence, les Nouvelles - Journal of the Licensing Executives Society, Volume LII No. 4, September 2017. Available at SSRN: https://ssrn.com/abstract=3009423. 237-240. 237.
[520] Marketa Trimble, Artificial Intelligence and Human Intelligence, GRUR International, Volume 72, Issue 1, January 2023, Pages 1–2, https://doi.org/10.1093/grurint/ikac109. 1.

rétegjei szorulhatnak fokozott mértékben az MI megoldások támogatására, akár a napi munkájuk során, akár az élet más területein.

Emellett az MI alkalmazása diszkriminációs problémákhoz is vezethet, ugyanis a nem megfelelő tanulási minták átvétele és a nagyfokú automatizáció révén az MI bizonyos személyekre vagy meghatározott társadalmi csoportokra nézve hátrányosabb döntéseket hozhat. Aggályokra adhat okot az az immáron számos vállalat esetén megjelenő gyakorlat, amely MI alkalmazásával 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.[521] A fentiekhez hasonlóan számos vállalat esetén MI eszközöket használnak a jelentkezők előszűrésére, így számos jelentkező el sem jut addig, hogy egy ember döntsön a sorsáról.

A fentiek kapcsán az EU-n belül a GDPR korlátozza azon eseteket, amikor az érintettre joghatással járó, vagy őt hasonlóképpen jelentős mértékben érintő eseteket automatizált döntéshozatal útján hoznak meg.[522] 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.

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 be már automatizált toborzási eszközökkel kapcsolatos szabályozást a fentebb írtak szerint. Az amerikai szabályozás az MI toborzási, valamint egyébként munkahelyi alkalmazása során jelentős hangsúlyt helyez a munkahelyi diszkriminációra, illetve az az elleni küzdelemre, amely az MI alkalmazása esetén a gyakorlatban kihívást jelenthet, tekintettel arra, hogy az MI 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 megoldások kapcsán

[521] Worker Info Exchange, Just Beat It! How Just Eat Robo-fires its Workers, 2023. április, https://www.workerinfoexchange.org/just-eat-report [2023.08.25.]. 1.
[522] GDPR 22. cikk (2) bek.

elfogultsági ellenőrzés („*bias audit*”) elvégzését írja elő legalább évente, amellyel az automatizált döntéshozatal során érvényesülő diszkrimináció csökkenthető.[523]

A toborzás mellett természetesen egyre jelentősebb szerepet játszik az MI a munkahelyi ellenőrzés során (például: internet- és email fiók használat ellenőrzése). A munkahelyi ellenőrzés 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,[524] 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. 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.[525] Arányosnak tekinthető azonban, ha a munkáltató például arányos, fokozatos lépések útján indokolt esetben (például: jogsértés gyanúja, közérdekű bejelentést követő vizsgálat) ellenőrzi a munkáltató internet-, informatikai eszköz-, illetve e-mail fiók használatát. Ez esetben is azonban a jogsértés megállapítása vagy kizárása érdekében fokozatos intézkedéseket szükséges alkalmaznia (például: jogsértő programok nagy mennyiségű letöltésének gyanúja esetén az adatforgalom ellenőrzése első körben). A munkáltatónak továbbá a munkahelyi internethasználat biztosítása és szabályozása során is ajánlott olyan intézkedéseket meghoznia, amelyek mind az esetleges jogsértéseket és visszaéléseket, mind az ellenőrzés szükségességére alapot adó esetek számát csökkentik (például: kockázatos weboldalak hozzáférhetőségének korlátozása).[526] Kiemelendő továbbá, hogy amennyiben a munkáltató MI alapú megoldást alkalmaz a munkahelyen, úgy ennek kapcsán elsődleges cél a munkáltató hálózatának, rendszereinek, valamint az azon tárolt információknak a védelme kell, hogy legyen. 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

[523] NY Local Law 144, § 5-301
[524] Bărbulescu v. Románia 61496/08. sz. ügy
[525] 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 [2023.09.01.]. 69.
[526] Uo.

átvizsgálása szükséges), úgy a munkáltatónak az alkalmazás során elsődlegesen a jogsértő esetek (például: kulcsszavas keresés alapján a jogsértést feltételező kifejezéseket tartalmazó e-mailek azonosítása) kiszűrésére kell fókuszálnia, mielőtt az érintett azonosításra, illetve vizsgálat alá vonásra kerülne.

A fentieken túl kiemelt szempontot képvisel továbbá az érintettek megfelelő tájékoztatása, amely révén az érintettek tudomást szerezhetnek az ellenőrzés lehetőségéről, valamint adataik kezeléséről, kapcsolódó jogaik gyakorlásáról. Ennek hiányában ugyanis az esetleges rejtett vagy meglepetésszerű, illetve a munkavállaló joggyakorlásának korlátozásával járó ellenőrzés jogsértőnek minősül. Ennek kapcsán szintén jelentős segítséget jelenthet megfelelő belső szabályzatok bevezetése, amelyek például a munkáltató által biztosított eszközök, alkalmazások használatára vonatkozóan tartalmaznak szabályokat. Ezen szabályzatok azonban értelemszerűen nem helyettesíthetik a megfelelő tájékoztatást vagy általában az adatvédelmi követelményeknek történő megfelelés biztosítását a munkahelyen, tekintettel arra, hogy ezen munkáltatói szabályzatok sokszor csak zártabb körben érhetők el, és azok megszövegezésébe, érvényesülésébe a munkavállalók igen korlátozott beleszólással rendelkeznek, így azok kapcsán jellemzően a munkáltatói érdek túlsúlya dominál.[527]

iii. A mesterséges intelligencia alkalmazása az online platformokon

Az MI a fenti területek mellett a közösségi médiaoldalakon és más platformokon is egyre jelentősebb szerepet tölt be. Az MI szerepe a közösségi médiaoldalakon kiterjed például a tartalomgyártásra, a tartalomszabályozásra- es moderálásra, valamint a marketingkampányok menedzselésére es a brand védelemre.[528] Maguk a platformok is napjainkra egyfajta összetett, általánosnak tekinthető kontrollmechanizmussá váltak, amelyek számos egyéb koordinációs mechanizmust felváltva, komplex szabályozási és intézkedési rendszer keretében működnek, az MI által támogatottan.[529]

[527] Balogh Zsolt György, Polyák Gábor, Rátai Balázs, Szőke Gergely László, Munkahelyi adatvédelem a gyakorlatban, Infokommunikáció és jog, 2012/3. 95-104. 96.
[528] 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/ [2023.08.28.]
[529] Ződi Zsolt, Algoritmikus koordináció a platformuniverzumban. A platform mint új koordinációs mechanizmus és ennek jogi következményei. In: Török Bernát és Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021. 491-521. 492.

Az MI alkalmazásával kapcsolatban napjainkban azonban a legjelentősebb kritika általában a tartalomszűréshez használt algoritmusokat éri. Ez kiterjedhet az egyes tartalmak felhasználók számára, célzott módon való megjelenítésére, a tartalmak szűrésére es korlátozására, akar az azt közzétevők tudta nélkül. Mindez számos jogi es etikai aggályt is felvet. Így a tartalomszűrési gyakorlat diszkriminációs aggályokat is felvethet, mivel az algoritmusok gyakran fejlesztőik meglévő nézeteit, előítéleteit hordozzák, amelyek igy az MI automatizált gyakorlata útján átfogó, diszkriminatív gyakorlat kialakításához vezethetnek.[530] 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.

A fentieken túl az MI marketing tartalmak es fizetett hirdetések megjelenítésével kapcsolatos gyakorlata is sok szempontból aggályosnak tűnhet, ennek révén ugyanis a felhasználókhoz sok esetben átláthatatlan módon, illetve forrásból jutnak el személyre szabott reklámtartalmak, igy a fogyasztót ügyleti döntések befolyásolására sarkallva, anélkül, hogy átláthatná a kapcsolódó lehetőségeit, valamint azt, hogy miért jutott el hozza az adott ajánlat.

A fenti problémák kapcsán megoldást jelenthet az algoritmusok alkalmazását megelőző átfogó hatásvizsgálat végzése, 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 legalább 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 szamara való elérhetőségét.

5. A mesterséges intelligencia általi adatkezelés az Amerikai Egyesült Államokban

Az MI szabályozása jelentős utat járt be az Egyesült Államok területén. Az elmúlt években az amerikai kormányzat felismerte az MI gazdasági és társadalomformáló szerepét, és határozott irányként tűzte ki az MI területén a vezető szerep megszerzését a világgazdaságban, amelyhez

[530] 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/ [2023.08.28.]

megfelelő szabályozási törekvés is társul. Így az amerikai szabályozás területén mind kormányzati, mind tagállami szinten történtek előre lépések, bár értelemszerűen az állami szabályozás dinamikusabbnak, egyúttal sokszínűbbnek is tekinthető.

Az alábbiakból az amerikai szövetségi szintű, illetve tagállami MI szabályozást foglaljuk össze, valamint kiemeljük a bírósági gyakorlat egyes szempontjait, hangsúlyosabbnak tekinthető döntéseit. Ismertetjük továbbá azzal kapcsolatos meglátásainkat, hogy megfelelő mintaként szolgál-e az európai szabályozás az amerikai számára, valamint, hogy meríthet-e az európai szabályozás az amerikaiból.

a. Az amerikai szabályozás és bírósági gyakorlat

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 képezik.

Szövetségi szinten az MI szabályozása szempontjából meghatározónak tekinthető a 2021-ben elfogadott National Artificial Intelligence Iniatiative Act,[531] amely egyrészt elfogadja az amerikai nemzeti MI stratégiát képező National Artificial Intelligence Initiative-et,[532] amely egyben az MI stratégiai pillérjeit is meghatározza, ideértve például az innovációt vagy az egyes kiemelt szakterületeket, mint például az egészségügyet.[533] A fentieken túl értelemszerűen az adatkezelést szabályozó rendelkezések jellemzően az MI általi adatkezelésre is kiterjednek, ideértve például az egészségügyi vagy a banki, illetve a pénzügyi szolgáltatók általi adatkezelésre vonatkozó szabályozást. Emellett a már fentiek szerint ismertettek szerint az algoritmusok általi diszkriminációval szembeni küzdelem is jelentős szabályozási célnak tűnik, amely tükrében a kialakulóban lévő szabályozás vélhetőleg más országok számára is meghatározó lesz majd.

[531] National Artificial Intelligence Act of 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210 [2023.09.03.]
[532] National Artificial Intelligence Initiative, https://www.ai.gov/ [2023.09.03.]
[533] Necz [353]. 113.

Az MI általi adatkezelés szabályozásával kapcsolatban azonban kifejezetten a tagállami szabályozás mondható jelentősnek. Az MI általi adatkezelésre vonatkozóan a tagállami jogszabályok különösen az európai szabályozáshoz hasonló rendelkezéseket tartalmaznak. Így például a kaliforniai szabályozás is a GDPR-hoz hasonlóan határozza meg az automatizált döntéshozatal fogalmát,[534] emellett szintén a GDPR-hoz hasonlóan határoz meg az automatizált döntéshozatallal járó technológiával, illetve profilalkotással kapcsolatos adatkezeléssel szemben való tiltakozással kapcsolatos jogot, valamint az alkalmazott logikára, fogyasztóra kiható eredményekre vonatkozó információhoz való hozzáférésre vonatkozó jogot.[535]

Az utóbbi időben az amerikai bírói gyakorlatban is megszaporodtak az MI megoldások alkalmazásával kapcsolatos ügyek. 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.[536] 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.[537] Egy másik ügyben, 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 jogát, valamint a biometrikus adatok 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.[538]

[534] CCPA 1798.140(z)
[535] CCPA 1798.185(16). Az egyes tagállami szabályozásokkal kapcsolatban lásd továbbá: Necz [353]. 114-115.
[536] 3:23-cv-3440. sz. ügy, keresetlevél, https://fingfx.thomsonreuters.com/gfx/legaldocs/myvmodloqvr/GOOGLE%20AI%20LAWSUIT%20complaint.pdf [2023.09.01.]
[537] https://clarksonlawfirm.com/wp-content/uploads/2023/06/0001.-2023.06.28-OpenAI-Complaint.pdf [2023.09.02.]
[538] ACLU v. Clearview AI, https://www.aclu.org/cases/aclu-v-clearview-ai [2023.09.02.]

A fentiekre tekintettel az amerikai szabályozás jelentős hangsúlyt fektet az automatizált döntéshozatal, valamint a profilalkotás szabályozására, azonban számos egyéb szempontot is érvényre juttat e téren, ideértve különösen a diszkrimináció elleni küzdelmet, valamint az átlátható adatkezelést. E tekintetben különösen a tagállami szabályozás tekinthető dinamikusnak. Emellett a bírói gyakorlat is dinamikusan fejlődik az MI általi adatkezelés tekintetében. Különösen a tesztadatok felhasználásával kapcsolatos bírói gyakorlat tűnik e tekintetben figyelemreméltónak, ahol az elmúlt időszakban indított perek és az azok végén hozott bírói döntések vélhetően meghatározók lesznek majd a jövő joggyakorlata számára is.

b. Megfelelő mintaként szolgálhat-e az európai szabályozás az amerikai számára?

A GDPR mint fő európai adatvédelmi jogszabály számos szempontból mintaként szolgál az EU-n kívüli államok szabályozása számára. Egyrészt letisztult fogalmi rendszert alkalmaz, másrészt keretrendszerként is szolgál számos kérdésben, ideértve például a jogalapok vagy az érintetti jogok meghatározását.

Az amerikai szabályozás is sok szempontból merít a GDPR szabályozási megoldásaiból és rendelkezéseiből, ideértve különösen a tagállami szabályozást, amely sok esetben támaszkodik az európai szabályozás definíciós készletére, valamint sok szempontból biztosít a GDPR-ban meghatározottakhoz hasonló érintetti jogokat. A fentebb írtak szerint a tagállami fogyasztói adatvédelmi jogszabályok egy része ugyancsak az európaihoz hasonlóan határozza meg az automatizált döntéshozatalt, illetve a profilalkotást, így a fogyasztói adatok kezelése esetén hasonló jogokat biztosít az MI általi adatkezelés által érintettek számára is.

Hangsúlyozandó azonban, hogy az amerikai szabályozás kevésbé tekinthető egységesnek, mint az európai. A szövetségi kormányzat jellemzően egyes kiemelt területeken alkotott adatvédelmi jogszabályokat (például: egészségügyi adatok kezelése), azonban ez esetekben is sokszor nagyobb „játékteret” biztosít a tagállami szabályozásnak, míg más területeken a tagállami szabályozás még aktívabb hajtóerővel bír (ideértve például a fogyasztói adatok kezelésével kapcsolatos szabályozást). Erre tekintettel eltérő kötelezettségek lehetnek irányadónak, az érintettek pedig eltérő jogokat élvezhetnek az egyes tagállamokban. Mindez persze nehézséget is jelenthet a számos tagállamban aktív vállalkozásnak, azonban az egyes tagállamokban érvényesülő szabályozások így a helyi szempontokat és érdekeket is nagyobb súllyal tudják

figyelembe venni. Emellett kiemelendő, hogy az egyes tagállami adatvédelmi jogszabályok jellemzően szűkebb kötelezetti kört határoznak meg, mint az európai adatvédelmi jogszabályok. Így például a CCPA hatálya is csak azon vállalkozásokra terjed ki, amelyek a) az adott naptári év január 1-ét megelőző naptári évben legalább bruttó 25.000.000 dollár éves árbevétellel bírnak, b) együttesen vagy külön-külön évente legalább 100.000 fogyasztó adatait vásárolják meg, adják el vagy osztják meg, vagy c) éves bevételül legalább 50%-a származik fogyasztók személyes adatainak eladásából vagy megosztásából.[539] Erre tekintettel a szabályozás körén kívül esnek az eseti szempontból adatértékesítéssel foglalkozó, illetve az ilyen tevékenységet végző kis- és középvállalkozások.

Az aktív bírói gyakorlat ugyancsak jelentős löketet ad az MI általi adatkezeléssel kapcsolatos jogalkalmazásnak, és segít kirajzolni az MI fejlesztéséhez és alkalmazásához szükséges adatok kezelésével kapcsolatos megfelelő jogalkalmazási környezetet. Ugyanakkor meglátásaink szerint e tekintetben különösen az etikusnak tekinthető MI megoldások fejlesztéséhez való felhasználás számára bővebb lehetőségeket kell hagynia mind a szabályozásnak, mind az angolszász területen kiemelt fontossággal bíró bírói gyakorlatnak, abból a célból, hogy a tudományos kutatásoknak és a fejlesztéseknek a túlzott peres kitettség ne képezhesse gátját.

c. Meríthet-e az európai szabályozás az amerikai szabályozás vívmányaiból?

A digitalizáció és az adatvédelem területén naponta merülnek fel újabb és újabb kérdések, amelyekre a jogalkotó számos esetben eltérő társadalmi viszonyokra és meghaladott technológiai környezetre szabott megközelítést igyekszik alkalmazni. Természetesen a technológiai fejlődés ténye önmagában nem ad alapot már kiforrott alapelvek és alapvető erkölcsi és jogi keretrendszerek felszámolására, vagy újragondolására, a digitalizáció és az MI szabályozása kapcsán azonban más területeknél nagyobb fokú rugalmasság látszik szükségesnek, amely a technológia fejlődését és alkalmazását is hatékonyan képes lekövetni.

Mindez álláspontunk szerint nem jelenti a technológiasemleges szabályozási megközelítés minden esetben való feladását, hiszen arra a jogviszonyok jelentős része esetén szükség van, azonban számos digitalizációval kapcsolatos jelenség és megoldás újfajta szabályozást vagy a meglévő szabályok új szemlélettel való alkalmazását kívánja meg. Álláspontunk szerint e

[539] CCPA 1798.140. (d) (1)

tekintetben az Egyesült Államok szabályozása rugalmasabban látszik reagálni, mint az európai. Míg ugyanis az előbbi esetén a szövetségi szabályozás alapvető keretein túl a tagállami szabályok sok szempontból dinamikusabb szabályozói választ képesek adni, úgy az európai tagállamok szabályozása jellemzően – akár sok éves késéssel is –, de bevárja a közösségi szabályozást, ez által számos esetben bizonytalan helyzetben hagyva a jogalkalmazókat. E tekintetben jó példaként tekinthető az európai hírközlési adatkezeléssel kapcsolatos szabályozás, amely hosszú évek óta próbál új európai uniós rendeletet alkotni, leváltva az adott terület több mint húsz évvel ezelőtti, meghaladott szabályozását.

Természetesen azonban az amerikai szabályozás rugalmassága egyben a hátrányaként is felfogható, tekintettel arra, hogy az egyes tagállamok szabályozása egy foltozott szőnyeg mintázatát adja, amelyben a szövetségi szabályozás sok szempontból csak keretjelleggel érvényesül, és legfeljebb egy-egy kérdésben hoz létre az Egyesült Államok teljes területén egységesen érvényesülő szabályozást. Mégis, ez a szabályozási környezet az, ahol a tagállami szabályozás dinamikusan képes érvényesülni és tovább-fejlődni, emellett a bírói gyakorlat is aktívan, jogformáló erővel hat a digitalizáció és az MI általi adatkezelés kérdésében. Emellett sok esetben szintén az amerikai szabályozás előnyének tekinthető annak specifikus jellege, amely szintén további gyors reagálóképességet biztosít a tagállami szabályozás számára (ideértve például a munkahelyi adatkezelés vagy a fogyasztói adatkezelés fentebb tárgyalt eseteit).

Meglátásaink szerint az amerikai szabályozás különösen a gyors reagálóképessége és specifikus, valamint piacközpontú jellegéből adódóan szolgálhat mintaként az európai szabályozás számára. Ennek hátrányaként tekinthető az alacsonyabb védelmi szint, azonban piacközpontúsága és a tagállami szabályozásból adódó dinamika okán az amerikai szabályozás a digitalizáció és az MI szabályozásának területén számos kérdésben látszólag gyorsabban képes reagálni, mint az európai.

Az európai szabályozás vívmányai a digitalizáció és az adatvédelem területén megkérdőjelezhetetlenek. Emellett az MI Rendelet Tervezet is vélhetőleg mintaszabályozásként szolgál majd az EU-n kívüli országok számára az MI szabályozása területén. Fontosnak tartjuk azonban leszögezni, hogy az amerikai szabályozás dinamikája, valamint egyes kérdésekben az amerikai szabályozásban megjelenő vívmányok (például: az MI általi diszkriminációval szembeni intézkedések) példaértékkel bírnak, a nemzetközi és európai

szabályozásban kialakított értékekkel és jó gyakorlatokkal ötvözve pedig egy fejlett és hatékonynak mondható technológiai szabályozási környezet kialakításához vezethetnek.

6. A digitalizáció és az adatvédelem további kihívásai, az adatvédelmi szabályok újragondolása

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 fókuszáltunk, amelyek álláspontunk szerint különös társadalomformáló erővel bírhatnak a közeljövőben, és amelyekre napjaink adatvédelmi szabályozása, különösen az EU-n belül, jellemzően nehézkesen képes reagálni. A fentiek kapcsán meglátásaink szerint új szabályozói megközelítésre van szükség a deepfake technológia kapcsán, amely a társadalmi diskurzusra bír jelentős formálóerővel. Emellett ugyancsak jelentős kihívásnak látjuk a metaverzum és a kapcsolódó technológiák szabályozását, amelyek egy újfajta világba engednek betekintést, ahol a „való világ" szabályai nem, vagy jelentősen másként érvényesülnek. A demokratikus társadalmak szempontjából ugyancsak jelentős hangsúllyal bír az arcfelismerő rendszerek elterjedése és szabályozása, amelyek alapjaiban határozzák meg az egyén és a kormányzat viszonyát, valamint az egyén szabadságának kereteit.

a. A deepfake technológia adatvédelmi problémái

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 valós személyeket személyesítenek meg; a „deepfake" kifejezés pedig 2017 végén terjedt el az interneten, és első körben olyan felvételekre használták, amelyeken ismert emberek arcát illesztették pornográf tartalmakra.[540] A deepfake tartalmak azonban napjainkra egyéb területen is elterjedtté váltak. Továbbra is számos esetben használják a technológiát közszereplők kifigurázása vagy kritizálása céljából (például: a politikai humor

[540] 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 [2023.06.07.]

eszközeként vagy szatirikus tartalmak elkészítéséhez), azonban egyre gyakrabban használják a technológiát reklámcélból vagy szolgáltatások nyújtása kapcsán, illetve magáncélból is.

Sajnálatos módon továbbá a jogsértő felhasználással kapcsolatos esetek sem szűntek meg. Napjainkra pedig 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.[541]

A deepfake technológia kapcsán érdemes megjegyezni, hogy akár jóhiszemű felhasználásról (például: egy politikus nyilvános kijelentéseit parodizáló videóanyag készítése), akár rosszhiszemű felhasználásról, illetve visszaélésről van szó (például: az érintettet valamely szexuális vagy egyéb kompromittáló helyzetben feltüntető képi- vagy videóanyag), mindaddig személyes adatok kezelésére kerül sor, amely a deepfake technológiával készült tartalom útján valamely természetes személy azonosítható. E tekintetben annak sincs jelentősége, hogy az érintett a valóságban nem követett el olyan cselekményt vagy nem tett olyan kijelentést, amely az adott tartalom útján 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.[542] Ilyen esetekben azonban az adatkezelésre vonatkozó jogszabályi rendelkezéseknek is szükséges megfelelni.

Természetesen azonban 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 jellemzően a szólás- és véleménynyilvánítás szabadsága elsőbbséget élvez, különösen amennyiben a technológia alkalmazása közszereplők nyilvános szereplésére vagy közhivatal betöltőjének bírálhatóságára vonatkozik. Elsőbbséget élvez azonban a személyes adatok védelméhez fűződő jog, amennyiben közvitához,

[541] 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 [2023.09.04.]
[542] GDPR 4. cikk 1. pontja

közbeszédhez nem tartozó, különösen amennyiben rosszhiszemű, az érintett magánéletére fókuszáló tartalmakról van szó.

Az EU-n belül az MI Rendelet Tervezet EP Változata szintén szabályozza a deepfake tartalmak felhasználását. Így az ilyen tartalmak esetén megfelelő módon tájékoztatást kell nyújtani arról, hogy a tartalmat mesterséges generálták vagy módosították, és ahol lehetséges, a generáló vagy módosító személyéről is.[543] A deepfake tartalmak szabályozása kapcsán azonban az EU-n kívül is említhetők fejlemények. Így további pozitív példaként említhető Kalifornia állam szabályozása, ahol a deepfake tartalmak szabályozása kapcsán két törvény is született. Az AB 730 törvény a politikai választások jogsértő befolyásolására használt tartalmakra vonatkozik (ideértve félrevezető, jogsértő tartalmak közzétételét választási befolyásolás céljából),[544] míg az AB 602 törvény a rosszindulatú, pornográf deepfake tartalmak felhasználása ellen vezet be szabályokat.[545] Emellett az Egyesült Államokban jellemzően a deepfake tartalmak hasonló, káros felhasználása személyiségi jogsértéssel is járhat, ideértve például a becsület, a magánszféra vagy „image jogok" (angolul: „*right to publicty*") megsértését.[546]

b. A virtuális valóság, a kiterjesztett valóság és a metaverzum adatvédelmi szempontjai

A virtuális valóság (angolul: „*virtual reality*", röviden: „*VR*") egy olyan mesterségesen létrehozott, virtuális környezetnek tekinthető, amely hardware eszközökkel érhető el, és amely a felhasználót ezen virtuális környezetbe helyezi.[547] A közelmúltban számos technológiai nagyvállalat, valamint egyéb vállalkozás és szervezet alakított ki a felhasználók által látogatható virtuális környezeteket, valamint tervezett ezek eléréséhez szükséges eszközöket (például: VR szemüveget vagy egyéb a fenti környezetben való interakciók végzéséhez szükséges eszközöket), így napjainkra egy komplex iparág épült ki, amely számos célt szolgálhat, valamint felhasználói igényt elégíthet ki. Ilyennek minősülhet például a tájékozódás, a szórakozás és különböző online játékok kiélvezése, de a VR eszközök és virtuális terek egyre

[543] MI Rendelet Tervezet EP Változata, 52. cikk 3. pontja
[544] Assembly Bill No. 730, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 [2023.09.04.]. Ezen jogszabály megújítás hiányában 2023. január 1. napjáig volt hatályban (section 1. 35. (b)).
[545] Assembly Bill No. 602, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB602 [2023.09.04.]
[546] Jason Haas, Deepfake dilemma, Intellectual property magazine, 2044-7175. (2019. September). 33-34. 33.
[547] Virtual Reality in the Classroom, University of Toronto, Ontario Institute for Studies in Education, https://guides.library.utoronto.ca/c.php?g=607624&p=4938314 [2023.06.11]

inkább teret nyernek például az oktatás és a kultúra területén. 2018-ban például a brit National History Museum a Sky VR Studio nevű céggel karöltve teremtett meg egy virtuális túrát, ahol a látogatók jelenlegi és rég kihalt állatokkal, valamint a múzeum kapcsolódó tárlatával is megismerkedhetnek, mindezt a híres brit természettudós, Sir David Attenborough vezetésével.[548]

A virtuális valósággal szemben az ún. kiterjesztett valóság (angolul: „*augmented reality*", röviden: „*AR*") a való világ kiterjesztése interaktív, digitális vizuális és egyéb elemekkel (például: hang).[549] Erre jó példának tekinthető a 2010-es évek közepén népszerűvé vált Pokémon Go játékapplikáció, amely esetén az okostelefon kamerájával, a való világban lehet érzékelni és befogni a virtuálisan megjelenő Pokémon szörnyecskéket.[550] Amellett, hogy az AR is jelentős lehetőségeket kíván számos iparág számára, valamint a szórakozás és a kikapcsolódás területén is, azonban alkalmazása során számos adatvédelmi kockázat is felmerül. Az ilyen alkalmazások esetén ugyanis a felhasználók jellemzően hajlamosabbak személyes adataik megadására és az eszközeikhez való hozzáférés engedélyezésére, a felhasználói adatok gyűjtésének pontos célja, illetve ezen adatok további felhasználása, valamint más szervezetekkel történő esetleges megosztása pedig a felhasználók számára számos esetben átláthatatlan marad.

A VR és AR alkalmazásokhoz képest a metaverzum jellemzően a felhasználók még nagyobb bevonására, valamint intenzívebb adatgyűjtésre épít, így ennek biztosítása kapcsán is értelemszerűen számos adatvédelmi kérdés merülhet fel, azonban ezek megválaszolásához elsőként szükséges tisztázni a metaverzumban kezelt adatok felhasználókhoz való viszonyát. Mindez azért is fontos, mert a metaverzumon belül, az adott virtuális világban a felhasználók nem közvetlenül, hanem jellemzően egy virtuális karakteren (avatár) keresztül jelennek meg, amelyhez egy felhasználónév társul. Ezen avatár ugyan bizonyos jellemzők tekintetében hasonlíthat a „valós" felhasználóhoz (például: hajszín, kedvelt öltözködési stílus), azonban jellemzően az avatár által nem azonosítható. Az érintettet általában a felhasználóneve sem

[548] Katie Pavid, Explore the Museum's collection with Sir David Attenborough, Natural History Museum, first published: 2018.03.06, https://www.nhm.ac.uk/discover/news/2018/march/explore-the-museum-with-sir-david-attenborough.html [2023.06.11.]
[549] Microsoft Dynamics 365, What is augmented reality or AR?, https://dynamics.microsoft.com/en-gb/mixed-reality/guides/what-is-augmented-reality-ar/ [2023.09.04.]
[550] Om Malik, Pokémon Go Will Make You Crave Augmented Reality, The New Yorker, Annals of Technology, 2016.07.12, https://www.newyorker.com/tech/annals-of-technology/pokemon-go-will-make-you-crave-augmented-reality [2023.09.04.]

azonosítja közvetlenül, tekintettel arra, hogy ez jellemzően a felhasználó teljes nevétől eltérő elnevezés (például: fantázianév vagy a keresztnév becézett alakja, illetve becenév). Mindemellett azonban az adott világ üzemeltetője és az annak kapcsán egyes szolgáltatást nyújtók (például: az adott világon belüli egyéb szolgáltatásokat nyújtó személyek vagy szervezetek) hozzáférhetnek a felhasználók személyes adataihoz (például: számlázási és fizetési adatok), amellett, hogy az avatárukra vonatkozó információkat is kezelnek, amelyek a felhasználót azonosító információkkal való együttes kezelésük esetén már személyes adatoknak tekinthetők.

Mindemellett azonban a metaverzumon belül számos egyéb adatkezelési művelet is elképzelhető, ideértve különösen a felhasználók által végzett adatkezelési műveleteket. Jellemzően ennek során is a fenti logika érvényesül. Így amennyiben az adott felhasználó csak más felhasználók avatárját kezeli (például: egy adott világon belüli eseményt streamel vagy oszt meg más avatárokat is ábrázoló képeket közösségi médiaoldalán), úgy ez nem tekinthető személyes adatok kezelésének, feltételezve, hogy az érintett avatárok mögött álló felhasználók nem kerülnek ezáltal azonosításra. Amennyiben azonban az avatárra vonatkozó információk mellett a felhasználó adatai is kezelésre kerülnek (például: az adott felhasználó hangjának rögzítésére is sor kerül a felvételen), úgy ez már személyes adatok kezelésével jár, amelyek kapcsán az adatvédelmi jogszabályi követelmények irányadónak tekintendők.

Természetesen azonban a fentieken túl is előfordulhat olyan eset, ahol pusztán az avatárhoz kapcsolódó információk kezelése során személyes adatok kezelése valósul meg. Így például, ha a fentebb írtakkal összhangban, az avatár neve a felhasználó nevével egyezik, vagy a felhasználót az avatár egyéb jellemzői egyértelműen azonosítják és a felhasználóhoz kötik (például adott esetben a felhasználó egyedi viseletének, tetoválásának és egyéb ismertetőjegyeinek viselése). Mindezen körülmények azonban természetesen esetről-esetre vizsgálandók, az adott eset valamennyi releváns jellemzőinek figyelembevételével (például: mennyire azonosítható kizárólag az érintett az avatár egyedi jellemzői által, mennyire „készíthet” más is hasonló avatárt). Megemlítendő továbbá, hogy amennyiben a technológia egy magasabb szintjén az érintettek tudatára vonatkozó, illetve abból származó információkat is képes kezelni az adatkezelő (például: meghatározott szenzor útján), úgy ennek kapcsán is személyes adatok kezeléséről beszélhetünk, az ezzel kapcsolatban felmerülő esetleges

adatvédelmi kérdésekre, problémákra azonban a gyakorlat még nem adott egyértelmű válaszokat.[551]

A fentiekkel összhangban megállapítható, hogy a metaverzumban kezelt adatok személyes adat jellegének megítélésén túl az adatkezeléssel kapcsolatos szerepek azonosítása is sok esetben kihívásnak tekinthető. Az adott világ üzemeltetője jellemzően adatkezelőként fog eljárni, különösen olyan adatkezelések kapcsán, amelyek az adott világ üzemeltetéséhez szükségesek (ideértve például a felhasználók bejelentkezéshez használt és egyéb azonosító adatait, az adott világban kifejtett tevékenységüket). Szintén adatkezelőknek tekinthetők azok a szolgáltatók, akik saját érdekükben gyűjtenek és kezelnek bizonyos adatokat a felhasználókról (például: az adott világon belüli rendezvények szervezői vagy létesítmények üzemeltetői).

Természetesen a fenti szempontok mellett a metaverzumon belüli vagy annak kapcsán végzett adatkezelésekkel kapcsolatosan számos egyéb kérdés, illetve szempont is felmerül, amelyeket a jövő szabályozásának kell majd tisztáznia, ideértve az adattovábbítással kapcsolatos jogszabályi követelményeknek történő megfelelést. Ez azért is fontos, mert mind az adott világ üzemeltetői, mind az abban szolgáltatást nyújtók és felhasználók számos országból származhatnak, így – jogi értelemben – rövid időn belül is adattovábbítások bonyolult hálózata alakulhat ki például egy metaverzumban szervezett találkozó kapcsán.

A fentiekkel összhangban a metaverzum kapcsán ugyancsak érdekes kihívásnak tűnik az átlátható adatkezelés biztosítása, tekintettel arra, hogy a metaverzum üzemeltetése és az azon belül nyújtott szolgáltatás kapcsán számos adatkezelési folyamat képzelhető el, amelyek kapcsán még egységesnek tekinthető tájékoztatási gyakorlat nem alakult ki. A jövő szabályozásának szükséges lesz azonban olyan adatkezeléssel kapcsolatos tájékoztatási gyakorlatot kialakítania, amely rugalmasan reagál a metaverzumban zajló adatkezelési folyamatokra, és nem jár a felhasználói élmény romlásával vagy a szolgáltatások igénybevételének indokolatlan korlátozásával. Ennek kapcsán jelentős segítség jelenthet a több szinten biztosított tájékoztatási gyakorlat kialakítása. Így például elterjedt gyakorlattá válhat egy-egy metaverzumban történő eseményen vagy egy ott működtetett létesítmény bejáratánál a személyes adatok kezelésének és az érintettek jogainak lényegi összefoglalása, az adott létesítmény vagy esemény üzemeltetéséért, illetve szervezéséért felelős adatkezelő

[551] Dr. Paul Lambert, Who Owns What's Inside Your Head? Thoughts, Mind Data, Ownership and Future Battles Ahead, European Intellectual Property Review, 2020, vol. 42/3, 174-178. 175-176.

megnevezése, valamint azon hivatkozás megadása, ahol bővebb tájékoztatás érhető el a személyes adatok kezeléséről, valamint az érintettek jogairól. Ez tehát hasonlóan érvényesülhet, mint például a valós rendezvényenek vagy létesítmények kapcsán történő adatkezelési gyakorlat kialakítása során.

Szintén kihívásnak tekinthető napjainkban az érintetti jogok metaverzumban való gyakorlásának biztosítása. Az érintett ugyanis a metaverzumban jellemzően az avatárján keresztül, továbbá az adott világ üzemeltetőjével szemben a felhasználói fiókján keresztül gyakorolhatja jogait, így a szolgáltatóknak is olyan módon kell kialakítaniuk az érintett megkeresések kezelését, hogy azok az érintett jogok gyakorlását ténylegesen támogatni tudják, a felhasználói élmény aránytalan sérelme mellett. Így például egy metaverzumban szervezett rendezvényen létrehozhatók olyan pontok, ahol az érintett bővebb tájékoztatást kérhet vagy segítséget kaphat az érintetti jogainak gyakorlása kapcsán; az effajta jó gyakorlatok tehát például a valós rendezvényeken vagy létesítményekben követett adatvédelmi gyakorlatokat követhetik, és nyújthatnak segítséget az érintettek számára.

Az érintetti érdekek figyelembevétele kapcsán segítséget jelenthet a megfelelő hatásvizsgálati gyakorlat kialakítása. Az adatvédelmi hatásvizsgálat során ugyanis megfelelő módon azonosíthatók és felsorolhatók az érintettek jogait és érdekeit potenciálisan sértő vagy veszélyeztető körülmények, valamint az ezek megakadályozására, illetve enyhítésére tett intézkedések, és ezek észszerűen várható hatásai. Emellett adott esetben a közeljövő szabályozása egyéb hatásvizsgálati gyakorlatot és követelményeket is előírhat a metaverzumban, illetve annak kapcsán szolgáltatásokat nyújtó és adatokat kezelő vállalkozások részére.

A fentiekre tekintettel a metaverzum adatvédelmi szempontjai kapcsán különös kihívást jelent majd az érintett és az általa létrehozott avatár kapcsolatának értékelése, valamint ezen keresztül az érintetti jogok gyakorlása és hatékony támogatása, amelynek egyszerre kell a technológia rapid fejlődésével ütemet tartania, valamint az adatvédelmi megfelelést dinamikus módon, az érintettek érdekeinek megfelelő mértékű figyelembevételével biztosítania.

c. Az arcfelismerő rendszerek alkalmazása

A közterületei kamerarendszerek telepítése önmagában is számos előnnyel járhat a társadalom, illetve a lakosság számára, ideértve a biztonságos lakó- és munkakörnyezet garantálását, azonban értelemszerűen ennek kapcsán egyéb érdekek is felmerülhetnek, ideértve például az alapvető emberi jogok tiszteletben tartását.[552] Az arcfelismerő rendszerek lényegében a kamerarendszerek előnyeit és az alkalmazásukkal kapcsolatos kockázatokat is jelentős mértékben megnövelik. Az arcfelismerő technológia által támogatott közterületi kamerarendszerek ugyanis adott esetben képesek lehetnek azonosítani a hatóságok által keresett személyeket (például: súlyos bűncselekmények elkövetőit), azonban az ezzel kapcsolatos társadalmi ellenőrzés, valamint az esetleges téves azonosításból eredő károk jelentős visszhangot váltottak ki az elmúlt években, amelyek többek között a magánszférájába való aktívabb hatósági behatásre, illetve a társadalom demokratikus működését érő esetleges torzító hatásokra, valamint a diszkriminatív azonosítási gyakorlatokra hívták fel a figyelmet.

A technológia jelentősége okán azt az EU-n belül az MI Rendelet Tervezet is szabályozza. Így a távoli biometrikus azonosító rendszert akként meghatározva, mint „*olyan MI-rendszer, amely a természetes személyeket távolból azonosítja valamely személy biometrikus adatainak a referencia-adatbázisban szereplő biometrikus adatokkal való összehasonlítása révén, és anélkül, hogy az MI-rendszer felhasználójának előzetes tudomása lenne arról, hogy az adott személy jelen lesz-e és azonosítható-e*”.[553] A jogszabály továbbá a valós idejű távoli biometrikus azonosító rendszert akként határozza meg, mint „*olyan távoli biometrikus azonosító rendszer, amelyben a biometrikus adatok rögzítése, az összehasonlítás és az azonosítása jelentős késleltetés nélkül történik. Ez nemcsak az azonnali azonosítást foglalja magában, hanem az intézkedések kijátszásának elkerülése érdekében a korlátozott rövid késleltetéseket is*”,[554] míg a nem valós idejű biometrikus azonosító rendszert, mint „*a „valós idejű” távoli biometrikus azonosító rendszertől eltérő távoli biometrikus azonosító rendszer*”.[555]

Hangsúlyozandó, hogy még az MI Rendelet Tervezet a valós idejű távoli biometrikus azonosító rendszerek alkalmazását bűncselekmények potenciális áldozatainak felkutatása, egyes jelentős veszélyek, illetve terrortámadás megelőzése vagy egyes súlyos bűncselekmények elkövetőinek felderítése, lokalizálása, azonosítása, illetve büntetőeljárás alá vonása érdekében lehetővé tette

[552] Kiss Attila, A közterületi térfigyelő rendszerek szabályozásának kihívásai a magyar jogalkotásban és a jogalkalmazásban, Infokommunikáció és jog, 2011/4. 136-143. 136.
[553] MI Rendelet Tervezet 3. cikk 36. pontja
[554] MI Rendelet Tervezet 3. cikk 37. pontja
[555] MI Rendelet Tervezet 3. cikk 38. pontja

volna,[556] az MI Rendelet Tervezet EP Javaslata már ugyanaz szakasz kapcsán általános tilalmat rendel el, a fenti kivételek alkalmazása nélkül.

A fentiek mellett továbbá 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 eljárásokat és jelentős szankciókat.[557] 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.[558]

A fentiek kapcsán természetesen nehéz vitatni a technológia alkalmazásával járó jelentős társadalmi kockázatokat, továbbá nehéz meghúzni azt a határt, ahol az arcfelismerő 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 megfigyelés történik, az ezen területen elhaladó érintetteket pedig az MI akár viszonylag kisebb súlyú bűncselekményekkel összefüggésben is azonosíthatja. Mindez a társadalom számára jelentős kockázatokkal is járhat, ugyanis tömeges megfigyelést alapoz meg az „egyszerű" térfigyelő kameráknál kifinomultabb, komplexebb azonosítást, illetve értékelést lehetővé tevő megoldással. Erre tekintettel a fentiek kapcsán érthetőnek tekinthetők a technológia alkalmazásával kapcsolatos aggályok és a vonatkozó tilalom. Hangsúlyozandó azonban, hogy nem kizárólag a súlyos bűncselekmények

[556] MI Rendelet Tervezet 5. cikk (1) bek. (d) pontja
[557] Lásd: az adatkezelés ellenőrzésével foglalkozó fenti pontban a Clearview AI-al szembeni eljárások kapcsán írtak.
[558] NAIH-963-10/2022.

elkövetőinek vagy feltételezett elkövetőinek azonosítása lehet az egyetlen terület, ahol a technológia sikeresen alkalmazható. Így például eltűnt személyek, sérült vagy más magatehetetlen emberek is könnyebben megtalálhatók a 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).

Amennyiben az arcfelismerő technológia a jövőben bizonyos szűken meghatározott esetekben, megfelelő szabályozás, illetve garanciák biztosítása mellett alkalmazásra kerül, úgy ennek kapcsán a rendszer alkalmazását, illetve az elkövetők azonosítást adott esetben indokoló cselekményeken túl vélhetően a megfigyelt terület és használatának, látogatásának jellegzetességei is kiemelt jelentőséggel bírnak majd. Egyes kiemelt súlyú bűncselekményeknek ugyanis jellemzően nagyobb eséllyel következnek be bizonyos, az ilyen cselekményekkel kapcsolatba hozható helyeken. Így például terrorcselekmények elkövetésének esélye jelentősen nagyobb számos ember által gyakran látogatott helyeken (például: repülőterek, pályaudvarok), valamint társadalmi, politikai vagy kulturális szempontból meghatározó helyeken (például: egyes állami, vallási vagy egyéb nagy tömeget vonzó vagy az adott közösség életében meghatározó jelentőségű rendezvények).

A fentieken túl az ilyen rendszerek megfelelő szabályozását feltételezve 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.[559]

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

Az MI, valamint a digitalizáció újabb vívmányai kapcsán felmerülhet a kérdés, hogy szükséges-e a technológiai fejlődés tükrében újra gondolnunk a személyes adatok védelmét, illetve az ezzel kapcsolatos szabályozási megközelítést. Ennek kapcsán kétségtelennek tekinthető, hogy az MI és – gyakran az MI-vel kapcsolatba hozható – egyéb formabontó technológiák (például: 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 a tudományos-fantasztikus művek lapjain vagy a filmvásznon látott, azonban egyre kevésbé futurisztikusnak tűnő élethelyzeteket eredményezhet. Néhány évtizede például ki gondolta volna, hogy a nagy nyelvi modellek forradalmasítják majd a munkavégzést, valamint számos iparágat, vagy hogy egy MI-alapú megoldás is 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. 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. Erre a robbanásszerű fejlődésre nyilván a jognak is reagálnia kell, azonban ezt – egyéb területek szabályozásához hasonlóan – csak a technológiai változásokat követően, azokra reagálva teszi.

Természetesen egyes szabályozási megközelítések – sok szempontból helyesen, generálklauzulákat alkalmazva vagy épp technológiasemleges módon – az esetleges változásokra felkészülten próbálnak reagálni a fenti beláthatatlannak tűnő változásokra. A

[559] Necz Dániel, A mesterséges intelligencia belügyi és biztonsági célú alkalmazása, Necz, Dániel (2020) A mesterséges intelligencia belügyi és biztonsági célú alkalmazása. SCIENTIA ET SECURITAS, 1 (1). pp. 49-53. ISSN 2732-2688 (online). 49-53. 51.

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 az MI Rendelet Tervezet és annak későbbi változatai is specifikus szabályokat alkalmaznak az MI egyes alkalmazásaira, és az amerikai vagy más harmadik országbeli szabályozási modellek is sok esetben ezt a technológia-specifikus megközelítést követik (például: a deepfake technológia esetén).

A magunk részéről példamutatónak tekintjük továbbá az MI Rendelet Tervezet kockázatszempontú megközelítését, amely arányosan igyekszik reagálni az egyes MI-rendszerekre, valamint az azokkal kapcsolatos kockázatokra. Egy ilyen általános MI szabályozásnak azonban az adatvédelmi, szellemi tulajdoni és egyéb specifikus jogterületekkel is nagyobb összhangot kell mutatnia, amely napjainkban még nem teljesen biztosított, tekintettel arra, hogy a jog sem az EU-n belül, sem más harmadik országokban nem látszik megfelelő ütemben tartani a lépést a gyorsuló technológiai fejlődéssel szemben.

További enyhítés látszik szükségesnek az olyan területeken, ahol az MI és a digitalizáció történelmi lehetőségekkel kecsegtet, és a társadalom számára különösen jelentős eredményeket érhet el. Például további enyhítés látszik szükségesnek az MI tudományos kutatási célú, illetve egészségügyi alkalmazása területén, ahol a komplex szabályozás sok esetben az érintettek jogainak és érdekeinek védelme által indokolt mértéken is túlmutató akadályt képez. Erre például szolgálhatnak a kutatási célú adatkezelésekre irányadó szabályok. Az ilyen adatkezelések kapcsán az EU-n belül a GDPR is enyhítést biztosít,[560] azonban számos egyéb követelmény (például: a gyűjtött adatok minimalizálása, az adatok továbbításával kapcsolatos korlátozások) adott esetben az enyhítést célzó szabályok ellenére is jelentős korlátozást jelenthet a fenti célból gyűjtött adatok kezelése kapcsán. A digitális térben továbbá általában véve nehézkesen értelmezhetők a GDPR adattovábbításra vonatkozó követelményei, illetve az MI kapcsán számos egyéb jogszabályi követelmény alkalmazhatósága is kihívást jelent (ideértve például az átlátható adatkezelés megfelelő biztosítását). Mindez azért is fontos, mivel Európa kiemelkedő kutatóhálózatokkal rendelkezik, amelyek nagyobb mértékű bevonása az MI kutatásokba jelentős mértékben hozzájárulhatnak a fejlődéshez.[561] Ehhez hasonlóan

[560] Ideértve például a célhoz kötöttség (GDPR 5. cikk (1) bek. b) pontja) vagy a korlátozott tárolhatóság (GDPR 5. cikk (1) bek. e) pontja) tükrében.
[561] Palkó Tamás, A mesterséges intelligencia kutatása az Európai Unióban, Európai Jog 20/4, 2020. 15-22. 21.

természetesen az amerikai kontinens és egyéb területek, országok kutatóhálózatai is jelentős hozzájárulást nyújtanak az MI és az új technológiák fejlesztéséhez, az ezek közti megfelelő együttműködés biztosítása pedig számos esetben a teljes emberiség számára hasznos lehet, például: az MI egészségügyi, gyógyszerkutatások területén való felhasználása kapcsán, vagy akár más területeken.

Más esetekben azonban a szabályozás egyértelmű enyhítése helyett inkább annak inkább másfajta értelmezésére vagy gyakorlati szempontú „áthangolásra" van szükség, ideértve például az érintettek tájékoztatását is. A tájékoztatásnak természetesen minden esetben az érintett számára átlátható adatkezelést szükséges garantálnia, azonban szükségesnek látszik kialakítani egy olyan megengedhető megközelítést (különösen az MI általi adatkezelés területén), ahol a technológia alkalmazásával kapcsolatos „észszerűen várható bizonytalanságok" a tájékoztatás részét képezik. Például az MI orvosi célú alkalmazása esetén nem feltétlenül adható teljeskörű tájékoztatás arról, hogy az MI miért azonosított egy adott megbetegedést vagy miért jutott eltérő kutatási következtetésre. Mivel azonban a technológia alkalmazásának elmulasztása jellemzően károsabb eredményekhez vezetne az érintett beteg, illetve a kutatás résztvevője számára, így a megfelelő orvosi tájékoztatással ötvözve adott esetben a fenti bizonytalanságokkal együttes adatvédelmi tájékoztatás is elégségesnek kell, hogy legyen. Megemlítendő azonban, hogy a jövőben az MI alkalmazásával és az MI általi adatkezeléssel kapcsolatos átláthatóságra vonatkozó követelményeknek is egységesen kell érvényesülniük. Egyértelmű átláthatóságra vonatkozó követelmények hiányában ugyanis az érintett szolgáltatók, adatkezelők kell, hogy meghatározzák az átláthatóság kereteit, amely félreértésekre, valamint manipulációra is alapot adhat.[562]

A fentiek mellett a digitális térben a hozzájárulás is rugalmasabb módon kell, hogy kezelhető legyen, például az ezirányú rendszerek, hálózatok kialakításával, ahol az érintettek folyamatos jelleggel követhetik nyomon és alakíthatják hozzájárulásuk által érintett adatok, adatkezelési célok, adattovábbítási címzettek körét. E körben napjainkban főként a közösségi médiaszolgáltatók gyakorlata alkalmazza a leginkább a fenti megközelítést, azonban számos esetben az áltáthatóság részleges biztosításával, általános jellegű tájékoztatásra fókuszálva. E

[562] 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. 1-14. 10.

körben meglátásaink szerint a tájékoztatásnak is a hozzájárulás köréhez jobban szükséges illeszkednie, és az érintettek számára még gyakorlatiasabb információkat, példákat, illetve a joggyakorlással kapcsolatos szükséges körű segítséget nyújtva.

Álláspontunk szerint nagyobb szabályozási fókuszt szükséges helyezni a diszkrimináció tilalmára, valamint az MI társadalmi egyenlőség érdekében való alkalmazására, amely kapcsán napjainkban az amerikai szabályozásban megjelenő törekvések példaértékűnek tekinthetők, amelyek a későbbiekben mintaszabályozást is nyújthatnak más országok számára.

A fentiek tükrében meglátásunk szerint az MI, illetve különösen az MI általi adatkezelés szabályozásának jellemzően az alábbi szempontokra szükséges kiterjednie:

- az innováció és a fejlesztési lehetőségek, illetve ezek kapcsán az öntanulást támogató szabályozói megközelítés,
- a túlzott protekcionizmus elkerülése, ehelyett az innovációra és a lehetséges körű együttműködésre való koncentrálás az érintettek érdekében,
- az MI alkalmazásával, valamint a felhasznált adatokkal, alkalmazott technológiával kapcsolatos „arányos átláthatóság”, amely figyelemmel van az MI létrehozójának, valamint alkalmazójának érdekeire is,
- az érintetti joggyakorlás, valamint az érintetti érdekek fokozottabb figyelembevétele, az adott technológia, valamint alkalmazási mód sajátosságaira tekintettel (például: érintetti joggyakorlás beépítése az MI használatába, ha az az érintett érdekeit szolgálja),
- az MI létrehozója, valamint alkalmazója általi hatásvizsgálat végzése, valamint az MI alkalmazásának fokozatos figyelemmel kísérése,
- a diszkrimináció és más, az érintettek érdekeit aránytalan módon sértő megoldások alkalmazásának elkerülése,
- az adatbiztonság egy magas szintjének megkövetelése, figyelemmel az érintett adatok körére, valamint az érintettek érdekeire és elvárásaira,
- 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 természetesen a társadalom és az érintettek igényeit is figyelembe veszi, és e körben arányos és észszerű követelményeket támaszt az új

technológiák alkalmazóival szemben. E körben álláspontunk szerint a túlzott protekcionizmus is kerülendő. Az MI és az egyéb új technológiák területén értelemszerűen a jövőben is szükség lesz határon átnyúló, valamint számos régió szereplőit tömörítő fejlesztési projektekre, ezen technológiák sajátja továbbá, hogy alkalmazásuk nem köthető földrajzi határokhoz, így aránytalan lokalizációs kötelezettségek sem támaszthatók észszerűen velük szemben. Ugyancsak ajánlott lehet a különleges adatok (például: egészségügyi adatok) kezelése kapcsán rugalmasabb szabályok előírása. A GDPR jelenlegi rendelkezései[563] ugyanis olyan zárt rendszert képeznek, amelyek számos esetben nem biztosítanak lehetőséget az érintettek személyes adatainak – akár az érintettek érdekében végzett – kezelésére, vagy az adatkezelőket nehezen vagy nem alkalmazható kivétel-szabályok hivatkozására kényszerítik a különleges adatok kezelésének GDPR szerinti általános tilalma[564] alól. Így például tanácsos lenne az érintettel kötött szerződések teljesítéséhez, valamint szélesebb körű egészségügyi célú tevékenységek végzéséhez és szolgáltatások nyújtásához szükséges kivételeket lehetővé tenni a különleges adatok kezelésének tilalma alól (például: online nyújtott egészségügyi szolgáltatások biztosításához).

Meglátásunk szerint azonban az MI és a digitalizáció újabb vívmányai kapcsán az adatvédelmi követelményeknek ezen technológiák sajátosságaira tekintettel kell érvényesülnie. Így, különösen az MI esetén, az átláthatóság alapelve is csak arányosan érvényesülhet. Mindez azért is fontos, mert a nem megfelelő mértékű átláthatóság biztosítása annak hiányához hasonlóan, jelentős károkkal járhat, mind az érintettre, mind az adatkezelőre nézve, ideértve különösen

- az érintettekre ható túlzott információs terhelést (például: túl részletes tájékoztatás az alkalmazott technológiához kapcsolódó technikai információk részletezésével),
- az érintett számára pusztán „látszólag" hasznos információk nyújtása (például: az érintett számára nem hasznos információk, elérhetőségek megadása),
- az új technológiák, valamint a fejlesztés és kutatás területén való kiszámíthatatlanság nehéz megragadása (például ideértve az MI alkalmazása kapcsán jelentkező „fekete doboz" problémát),
- gazdasági vagy információbiztonsági érdekeket sértő információk, adatok felfedése (különösen, ha azok különösebben nem hasznosak az érintett számára).[565]

[563] Lásd: GDPR 9. cikk (2) bek.
[564] Lásd: GDPR 9. cikk (1) bek.
[565] Necz [353]. 15.

Ezen „arányos átláthatóságnak” elsősorban az érintettre járó vagy az érintett és a környezet számára releváns hatásokra kell fókuszálnia, a közérthetőségre és a technikai háttér túlzott bemutatásának elkerülésére figyelemmel, tekintettel arra, hogy a „túlzott” transzparencia vagy a nem közérthető, túlságosan technikai információk félrevezethetik az érintettet és erodálhatják a transzparens adatkezelés lényegét. A fentiek szerinti technológia környezetben értelemszerűen az érintetti joggyakorlás is jellemzően sajátosan foghat helyt. E körben álláspontunk szerint kiemelt hangsúllyal bír majd az adatkezelők érintetti jogok gyakorlását támogató kötelezettsége. Ezen kötelezettség értelemszerűen annál erősebb, minél gyengébb pozícióban van az érintett. Így például gyermekek, kórházi ellátásra szorulók esetén magasabb szintű támogatás várható el az adatkezelőtől, hiszen ezen személyek értelemszerűen kevésbé képesek jogaikat gyakorolni, érdekeiket érvényesíteni.

A fentieken túl álláspontunk szerint a szabályozásnak nagyobb figyelmet kell fordítania a diszkrimináció és a társadalom számára különösen negatív hatások, visszaélések kiszűrésére, és a magas fokú információbiztonságra. E körben azonban a követelményeknek kockázatalapú megközelítés szerint az adott rendszer vagy megoldás kockázatával arányos mérték szerint 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

A digitalizáció és az MI jelentős kihívás elé állítja a személyes adatok védelmét, ideértve a jelentős adatmennyiség felhalmozását, hasznosítását és az ezekre épülő gazdasági modelleket és új technológiákat.[566] Ezen új környezet azonban új lehetőséget is biztosít napjaink adatvédelmi szabályozásának gyakorlati értelmezése, felülvizsgálata, valamint a szükséges körű újragondolása tekintetében. Ennek kapcsán elsődlegesen az etikus technológia-használat elterjedését tekintjük szükségesnek, amely az adatvédelem és az etikus MI kapcsán felállított alapelvek tiszteletben tartását is magában foglalja, emellett azonban szintén szükséges olyan, innovációt támogató szabályozási környezet kialakítása, amely az érintettek szabadságain és

[566] Szőke Gergely László, Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és jog, 2013/3. 107-112. 110.

érdekein túl a szolgáltatók érdekeit, valamint az új technológiák biztosította lehetőségeket és előnyöket is figyelembe veszi.

A fentiek kapcsán azonban felmerül a kérdés, hogy szabályozható-e digitalizáció és az MI a fejlődés megakasztása nélkül, vagy a szabályozás szükségszerűen a fejlődés visszavetéséhez vezet. Álláspontunk szerint a szabályozásnak sem célja, sem eredménye nem lehet a digitalizációval és az MI-vel kapcsolatos fejlesztések és innováció visszavetése, azonban az etikátlan, valamint jogszabályi követelményeknek meg nem felelő rendszerek és megoldások értelemszerűen korlátozandók, ezek tekintetében ugyanis az esetleges további fejlesztések adott esetben csak tovább növelnék a kapcsolódó kockázatokat és aggályokat. Így amennyiben egy MI alapú megoldást társadalmi pontrendszer alkalmazása kapcsán fejlesztenek, úgy ezen megoldás újabb, még hatásosabb verziói csak további demokratikus aggályokat támasztanak, így az ezzel kapcsolatos fejlesztések nem számíthatnak a demokratikus jogalkotó támogatására. Ugyancsak kockázatos lehet például egy MI alapú rendszer bírósági döntéshozatal céljára való alkalmazása, ezen rendszerek kiterjedt bírósági alkalmazása ugyanis egy magasabb fejlettségi szinten is sértheti a tisztességes eljáráshoz való jogot.[567] Más esetekben azonban, ha a fejlesztés és az innováció képes az adott rendszer alkalmazásával kapcsolatos aggályokat kiküszöbölni vagy észszerűen kezelhető szintre csökkenteni, úgy ezen fejlesztések elé álláspontunk szerint nem gördíthetők észszerűtlen akadályok. A fentiek kapcsán megemlítendő azonban, hogy egy szabályozási verseny is kialakulhat egy-egy technológia kapcsán az egyes országok között. Ez a mintaszabályozások (például az adatvédelem területén a GDPR) kialakulásán túl egyben negatív hatásokkal is bírhat, adott esetben visszafogva a külföldi innovációt vagy a gazdasági és tudományos kapcsolatokat. Így az adott piac túlzott védelme vagy a határon átnyúló adattovábbításokat és együttműködést korlátozó intézkedések álláspontunk szerint kiküszöbölendők, és csak korlátozott esetekben tarthatók fenn (például: ha egy adott megoldás a demokratikus társadalmakban etikus módon nem használható vagy nemzetbiztonsági kockázatot jelent).

A fentiek kapcsán megemlítendő továbbá, hogy az egyes országok és régiók eltérő szabályozási technikákat alkalmaznak az adatvédelem és a digitalizáció, illetve az MI szabályozása területén, amelyek különböző mértékben hatnak a technológiai fejlődésre és az egyes technológiák

[567] 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, 2022, VIII/4. 7-38. 13.

alkalmazására. Az MI alkalmazásából eredő kockázatok azonban főként az MI öntanulási képességeiből erednek, illetve azokhoz kapcsolódnak, amely egyben a kockázatalapú szabályozási megközelítések magját is képezi.[568] Sőt, a félelmek egy része éppen az MI azon sajátosságához kapcsolódik, hogy – elvileg – képes lehet meghaladni az emberi értelem szintjét és az ember számára pótolhatatlan erőforrássá válni, vagy akár az ember számára jelentős károkat okozni, vagy az emberiséget fenyegetni.[569] Mindemellett az MI, illetve annak alkalmazásából eredő károk a gyakorlatban igen sokfélének tekinthetők (ideértve akár materiális vagy immateriális károkat is),[570] a jelen tanulmányban azonban elsődlegesen a személyes adatok kezelésére, és a jogsértő adatkezelésből származó esetleges károkra helyzetük a hangsúlyt. E tekintetben továbbá a tanulmányban főként az európai és az amerikai szabályozásra fókuszáltunk, tekintettel arra, hogy mind szabályozási, mind innovációs szempontból ezen szabályozásokat tekintjük mintaértékűnek, illetve globálisan a legjelentősebbnek.

Az európai szabályozás az MI szabályozása kapcsán kockázatalapú megközelítésből indul ki, amely az adott rendszer, illetve alkalmazása által jelentett kockázatok szerint támaszt tilalmakat vagy rendel követelményeket. Mindez az átfogó európai adatvédelmi szabályozással karöltve széleskörű védelmet biztosít az MI általi adatkezelés kapcsán, amely különös figyelmet helyez az átláthatóságra, az érintetti jogok gyakorlásának támogatására és biztosítására, valamint a megfelelő szintű adatbiztonsági intézkedések biztosítására. Emellett az európai jogalkotó a digitalizáció számos területén kiemelten aktívnak bizonyult az elmúlt években, jelentős szabályozást alakítva ki az online piacok, az online térben történő adatkezelés, valamint az MI és az új technológiák kapcsán.

Az európai szabályozás mellett sok tekintetben eltérő utat választott az amerikai szabályozás, amely átfogó adatvédelmi vagy MI szabályozással nem rendelkezik, e helyett egyes kiemelt súlyú területekre fókuszál szövetségi szinten (ideértve például a gyermekek adatainak kezelését az online térben, az egészségügyi vagy más szakterületeket érintő adatkezelést vagy az MI általi diszkriminációval szembeni küzdelmet). Emellett az egyes tagállamok szintjén igen aktív

[568] Ződi Zsolt, A mesterséges intelligencia szabályozásának dilemmái. 1. rész: A mesterséges intelligencia (jogi) definíciója, https://www.ludovika.hu/blogok/itkiblog/2020/08/24/a-mesterseges-intelligencia-szabalyozasanak-dilemmai/ [2023.09.29.]
[569] Négyesi Imre, A mesterséges intelligencia és az etika. Hadtudomány 2020/1. 103-113. 107.
[570] Tóth András, A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, Infokommunikáció és jog, 2019/2. 3-9. 3.

jogalkotás zajlik, amely számos területre fókuszál, ideértve különösen a fogyasztói adatok védelmét, a diszkrimináció elleni küzdelmet vagy a munkahelyi adatkezelést). Mindez természetesen egy európainál széttagoltabb amerikai szabályozási kultúrát eredményez, azonban az aktív bírói gyakorlattal karöltve egyfajta rugalmasságot is biztosít, amely a fejlődés motorját is képezi, rávilágítva az esetleges szabályozási gyengepontokra, hiányosságokra vagy épp az aktívabb szabályozás szükségességére.

Az MI szabályozásán és az MI általi adatkezelésen túl azonban a digitalizáció egyéb vívmányai is kihívások elé állítják a jogalkotót, valamint a jogalkalmazókat, ideértve például a metaverzumot és a kapcsolódó technológiákat, vagy például az MI adta lehetőségekre építő deepfake tartalmakat. Ezek a technológiák az általuk kínált számos lehetőség mellett ma még csak részben látható, illetve érthető kockázatokkal bírnak, amelyek kezelése – különösen a metaverzum tekintetében – nemzetközi választ követel meg, helyi, illetve régiós szinten e tekintetben jellemzően csak részleges válaszok adhatók.

A fentiekre tekintettel felmerülhet az a kérdés is, hogy szükséges-e újra gondolnunk a személyes adatok védelmét az MI és a digitalizáció újabb vívmányai kapcsán. Ennek kapcsán álláspontunk szerint teljesen új adatvédelmi szabályok kidolgozására nincs szükség, lévén, hogy a személyes adatok védelmével kapcsolatos alapelvek és alapvető követelmények az MI és a digitalizáció újabb vívmányai kapcsán is alkalmazhatók, szükséges azonban ennek kapcsán újfajta megközelítés alkalmazása, amely az egyes elvárásokat az adott technológiai környezetre és annak alkalmazására tekintettel érvényesíti (ideértve például az érintetti jogok adott környezetre és alkalmazásra tekintettel való megfelelő támogatását). Ennek kapcsán meglátásaink szerint egyfajta szabályozói és jogalkalmazói rugalmasság is elvárható, amely az adatvédelmi követelményeket az érintett jogaira, valamint érdekeire tekintettel, azonban az alkalmazás sajátosságainak figyelembevételével, a technológiai fejlődés megakasztása nélkül, és a technológia pozitív hatásainak támogatásával érvényesíti.

9. Irodalomjegyzék

Tudományos publikációk:

Alan Mathison Turing: Computing Machinery and Intelligence. Mind, 59. évf. 236. sz., 1950. október. 433-460. 433-434.

Balogh Zsolt György, Polyák Gábor, Rátai Balázs, Szőke Gergely László, Munkahelyi adatvédelem a gyakorlatban, Infokommunikáció és jog, 2012/3. 95-104.

Böcskei Balázs, Német Szilvi, Toxikus technokultúrák és digitális politika. Érzelmek, mémek, adatpolitika és figyelem az interneten, Napvilág Kiadó – TK PTI, 2021.

Brian Christian, The Most Human Human, Anchor Books, New York, 2011.

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, 37 MedR, 2019. https://doi.org/10.1007/s00350-019-5247-2. 431-439.

Chris Reed: Data Trusts for Lawful AI Data Sharing. In: Gary Chan Kok Yew, Man Yip (ed.): AI, Data and Private Law, Translating Theory into Practice, Hart Publishing, 2021. 47-68.

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, 2022, VIII/4. 7-38.

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, T.M.C. Asser Press The Hague, 2022. 187-204.

Cserván Csaba, A digitalizáció hatása az alapjogok hatására és érvényesítésére. In: Homicskó Árpád Olivér (szerk.), A digitalizáció hatása az egyes jogterületeken, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, Budapest, 2020, 55-76.

Davenport T, Kalakota R. The potential for artificial intelligence in healthcare. Future Healthc J. 2019 Jun;6(2):94-98. doi: 10.7861/futurehosp.6-2-94. PMID: 31363513; PMCID: PMC6616181.

David Erdos, European Data Protection Regulation, Journalism, and Traditional Publishers. Balancing on a Tightrope? Oxford University Press, Oxford, 2019, impression: 2. 193.

Deepa Ravindranath, A Guide to Commercial Innovation in Artificial Intelligence, les Nouvelles - Journal of the Licensing Executives Society, Volume LII No. 4, September 2017. Available at SSRN: https://ssrn.com/abstract=3009423. 237-240.

Domokos Márton, Gyakorlati tapasztalatok a GDPR-megfelelés során. In: Szabó Endre Győző (szerk.), Az Infotörvénytől a GDPR-ig, Ludovika Egyetem Kiadó, Budapest, 2021. 209-220.

Dr. Paul Lambert, Who Owns What's Inside Your Head? Thoughts, Mind Data, Ownership and Future Battles Ahead, European Intellectual Property Review, 2020, vol. 42/3, 174-178.

Eduard Fosch-Villaronga, Robots, Healthcare, and the Law. Regulating Automation in Personal Care, e-book version, 2020.

Elek István: Az intelligencia spontán megjelenése. ELTE Eötvös Kiadó, Budapest, 2015.

Forti, Mirko, The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR (June 27, 2021). European Journal of Legal Studies 13 (1), June 2021, 29-44, Available at SSRN: https://ssrn.com/abstract=3866576.

Freidler Gábor, A személyes adatok védelméhez való jog jelentése. In: Dósa Imre (szerk.): Az informatikai jog nagy kézikönyve, CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft, Budapest. 17-29.

Gyekiczky Tamás, Jogrendszerek a Digitális Társadalomban, Wolters Kluwer Hungary Kft., Budapest, 2020.

Hannah Fry, Emberek és gépek. Hogyan tartsuk a kezünkben az irányítást a mesterséges intelligencia korában? HVG Kiadó Zrt, Budapest, 2021. Fordította: Dembinszky Zsófia (2020), eredeti kiadás: 2018.

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. 1-14.

Hubert L. Dreyfus, What Computers Still Can't Do. A Critical of Artificial Reason, The MIT Press, Cambridge, London, 1992.

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

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, Routledge, London, 2021. 76-80.

Jane Kaye, Edgar A Whitley, David Lund, Michael Morrison, Harriet Teare, Karen Melham, Dynamic consent: a patient interface for twenty-first century research networks, 23 European Journal of Human Genetics, 2015. https://doi.org/10.1038/ejhg.2014.71. 141-146.

Jason Haas, Deepfake dilemma, Intellectual property magazine, 2044-7175. (2019. September). 33-34.

Joanna J. Bryson, Robots Should Be Slaves, January 2010, DOI:10.1075/nlp.8.11bry

John R. Searle, Minds, brains and programs, The Behavioral and Brain Sciences 3/1980, doi:10.1017/S0140525X00005756. 417-457.

Kiss Attila, A közterületi térfigyelő rendszerek szabályozásának kihívásai a magyar jogalkotásban és a jogalkalmazásban, Infokommunikáció és jog, 2011/4. 136-143.

Kis Kelemen Bence, Hohman Balázs, A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra, Infokommunikáció és jog, 2016/2. 64-70.

Klein Tamás, Robotok a beteggondozásban és a gyógyításban. In: Klein Tamás, Tóth András (szerk.): Technológia jog – Robotjog – Cyberjog, Wolters Kluwer Hungary, Budapest, 2018. 210-211.

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, Dialóg Campus Kiadó, Budapest-Pécs, 2009.

Ligeti Miklós, A közérdekű adatok megismerhetőségének buktatói, Infokommunikáció és jog, 2015/1. 26-30.

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 University Press, Edinburgh, 2020. 262-292.

Marketa Trimble, Artificial Intelligence and Human Intelligence, GRUR International, Volume 72, Issue 1, January 2023, Pages 1–2, https://doi.org/10.1093/grurint/ikac109.

Mark Owen, Maria Luchian, Following the AI path, Intellectual property magazine, 2044-7175. (September 2020). 15-16.

Marilena Garis, Meeting the challenges of digitalisation, Managing intellectual property, 0960-5002. issue 199. (2010). 88-90.

Miskolczi Barna, Szathmáry Zoltán, Büntetőjogi kérdések az információk korában – mesterséges intelligencia, big data, profilozás. Budapest, HVG-Orac Lap- és Könyvkiadó Kft., Budapest, 2018.

Miquel Peguera: The right to be forgotten in the European Union. In: Giancarlo Frosio (ed.): The Oxford Handbook of Online Intermediary Liability, Oxford University Press, Oxford, 2020, 486-502.

Nagy Zoltán András, Bűncselekmények számítógépes környezetben, Ad Librum, Budapest, 2009.

Necz Dániel: Az egyházak általi adatkezelés. In: Kiss Gábor (szerk.): Fiatal Kutatók és Doktoranduszok X. Nemzetközi Jubileumi Teológus-Konferenciájának Tanulmánykötete, Doktoranduszok Országos Szövetsége, Budapest, 2020. 415-425.

Necz Dániel, A mesterséges intelligencia adatvédelmi szempontjai, különös tekintettel a belügyi szervek adatkezelési gyakorlatára. https://bm-tt.hu/wp-content/uploads/2022/02/2020_1.pdf. 135-165.

Necz Dániel, A mesterséges intelligencia belügyi és biztonsági célú alkalmazása, Necz, Dániel (2020) A mesterséges intelligencia belügyi és biztonsági célú alkalmazása. SCIENTIA ET SECURITAS, 1 (1). pp. 49-53. ISSN 2732-2688 (online). 49-53.

Necz Dániel: A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai. Acta Humana – Emberi Jogi Közlemények, 10(3), https://doi.org/10.32566/ah.2022.3.4. 95-123.

Necz Dániel, A mesterséges intelligencia hatása a szerzői jogra, Iparjogvédelmi és Szerzői Jogi Szemle, 123/6 (2018). 51-76.

Négyesi Imre, A mesterséges intelligencia és az etika. Hadtudomány 2020/1. 103-113.

Palkó Tamás, A mesterséges intelligencia kutatása az Európai Unióban, Európai Jog 20/4, 2020. 15-22.

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, Edmund Elgar Publishing, Cheltenham, Northampton, 2020. 391-410.

Péterfalvi Attila, Algoritmusok és adatvédelem: Quo vadis? A 2020.02.27-i mesterséges intelligencia alkalmazásának hatása az alapjogokra című konferencián elhangzott előadás szerkesztett leirata, Török Bernát és Ződi Zsolt (szerk.), A mesterséges intelligencia

szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021, 179-185.

Révész Balázs, Az adatkezelés alapelvei. In: Péterfalvi Attila, Révész Balázs, Buzás Péter, Magyarázat a GDPR-ról, Wolters Kluwer Hungary Kft., Budapest, 2021. 103-121.

Ron Dolin, Technology Issues in Legal Philosophy. In: Daniel Martin Katz, Ron Dolin, Michael J. Bommarito (eds.), Legal Informatics, Cambridge University Press, Cambridge, New York, 2021. 5-23.

Szabó Endre, Az adatvédelmi tisztviselőről. A GDPR szabályainak elemzése, Infokommunikáció és jog, 2018/1. 3-10.

Szegedi László, Dornfeld László, Polgár Zoltán, Teleki Bálint, A GDPR alkalmazásával kapcsolatos első tagállami tapasztalatok – egységes szabályozás, eltérő alkalmazás? Infokommunikáció és jog, 2021/1. 10-16. 15.

Szőke Gergely László, Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és jog, 2013/3. 107-112.

Szűcs Gábor, Sallai Gyula, Az okos város kameraképeinek elemzése, Dialóg Campus Kiadó, Budapest, 2019.

Tóth András, A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, Infokommunikáció és jog, 2019/2. 3-9.

Udvary Sándor, Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései, Gazdaság és jog 2018/12. 14-21.

Ződi Zsolt, Algoritmikus koordináció a platformuniverzumban. A platform mint új koordinációs mechanizmus és ennek jogi következményei. In: Török Bernát és Ződi Zsolt (szerk.), A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021. 491-521.

Internetes hivatkozások:

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/

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

A megfelelő adatvédelmi szintet biztosító országok listájához lásd: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

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/

Anokhy Desai, US State Privacy Legislation Tracker, IAPP, utolsó felülvizsgálat: 2023.07.21., https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Arjun Kharpal, What is 'Web3'? Here's the vision for the future of the internet from the man who coined the phrase, CNBC, 2022.04.19, https://www.cnbc.com/2022/04/20/what-is-web3-gavin-wood-who-invented-the-word-gives-his-vision.html

Blagoj Delipetrev, Chrisa Tsinaraki, Uroš Kostić, AI Watch, Historical Evolution of Artificial Intelligence, Analysis of the three main paradigm shifts in AI, 2020, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120469/jrc120469_historical_evolution_of_ai-v1.1.pdf

Capitalizing on the data economy, MIT Technology Review Insights, 2021.11.16, https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/

ChatGPT, https://openai.com/blog/chatgpt

Commission appoints expert group on AI and launches the European AI Alliance, DIGIBYTE,

Európai Bizottság, 2018. június 14, https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance

Daniel G. Bobrow, Natural Language Input for a Computer Problem Solving System, 1964.03.01, https://dspace.mit.edu/bitstream/handle/1721.1/5922/AIM-066.pdf?sequence=2&isAllowed=y

Dario Casella, Laurence Lawson, AI and privacy: Everything you need to know about trust and technology, ericsson.com, 2022.08.01, https://www.ericsson.com/en/blog/2022/8/ai-and-privacy-everything-you-need-to-know

Deloitte, What is digital economy? https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

Democratizing AI: Satya Nadella on AI vision and societal impact at DLD, Microsoft, 2017.01.17, https://news.microsoft.com/europe/2017/01/17/democratizing-ai-satya-nadella-shares-vision-at-dld/

Digitális Szabadság Bizottság, https://digitalisszabadsag.kormany.hu/

Digitalization, Gartner Glossary, Gartner, https://www.gartner.com/en/information-technology/glossary/digitalization

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

Domokos Márton, Horváth Anna Zsófia, Dark patterns – napvilágra kerülő sötét megoldások, Jogi Fórum, https://www.jogiforum.hu/blog-ip-it-vedjegy-domain-internet-jogi-blog-11/2021/09/02/dark-patterns-napvilagra-kerulo-sotet-megoldasok/

Edith M. Lederer, UN council to hold first meeting on potential threats of artificial intelligence to global peace, AP News, Technology, 2023.07.03, https://apnews.com/article/artificial-intelligence-un-security-council-meeting-uk-f7fb6d8f8a261a9d9b23ca463ee29d3d

EDPS, Data Protection Officer (DPO), https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

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

Ellenőrző Bizottság, https://www.oversightboard.com/appeals-process/

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

Emily Reynolds, The agony of Sophia, the world's first robot citizen condemned to a lifeless career in marketing, Wired, Science, 2018.06.01, https://www.wired.co.uk/article/sophia-robot-citizen-womens-rights-detriot-become-human-hanson-robotics

Eric A. Taub, Sleepy Behind the Wheel? Some Cars Can Tell, The New York Times, 2017.03.16, https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html#:~:text=Through%20its%20Driver%20Availability%20Detection,drowsiness%20detection%20systems%20exist%20today

European Commission, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, 2019.01.23, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

European Commission, Smart cities, https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

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/

European Data Protection Supervisor, Internet of Things, https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en

Európai Tanács, Európai digitális egységes piac, Bevezetés, https://www.consilium.europa.eu/hu/policies/digital-single-market/

Everything You Should Know About the Dark Web, Tulane University School of Professional Advancement, https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web

Explainable AI, Google, https://cloud.google.com/explainable-ai

Facebook, Elhunyt személy fiókjának kezelése, https://www.facebook.com/help/275013292838654

Fact Check-Video does not show Joe Biden making transphobic remarks, Reuters, Reuters Fact Check, 2023.02.10, https://www.reuters.com/article/factcheck-biden-transphobic-remarks-idUSL1N34Q1IW

Gartner, Gartner Glossary, Non-Fungible Token (NFT), https://www.gartner.com/en/information-technology/glossary/non-fungible-token-nft

Gergely Szakacs, Hungary mulls sanctions against social media giants, Reuters, Technology News, 2021.01.18, https://www.reuters.com/article/us-hungary-media-regulations-idUKKBN29N1BV

Google AI, Our Principles, https://ai.google/responsibility/principles/

Google, Bard Experiment, https://bard.google.com/?hl=en

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

GPAI, https://gpai.ai/about/

GPDP, ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for european users and non-users, 2023.04.28, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490

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/

IBM, From principles to actions: building a holistic approach to AI governance, https://www.ibm.com/blog/from-principles-to-actions-building-a-holistic-approach-to-ai-governance/

IBM, What is blockchain technology? https://www.ibm.com/topics/blockchain

Information Commissioner's Office, When can we refuse to comply with a request? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/when-can-we-refuse-to-comply-with-a-request/

Jamie Grierson, Photographer admits prize-winning image was AI-generated, The Guardian, Culture, 2023.04.17., https://www.theguardian.com/technology/2023/apr/17/photographer-admits-prize-winning-image-was-ai-generated

Jane Wakefield, Deepfake presidents used in Russia-Ukraine war, BBC News, 2022.03.18, https://www.bbc.com/news/technology-60780142

John Edwards, Bitcoin's Price History, Investopedia, 2023.05.24, https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp

John McCarthy, What is Artificial Intelligence? http://www-formal.stanford.edu/jmc/whatisai/node1.html

Katie Pavid, Explore the Museum's collection with Sir David Attenborough, Natural History Museum, first published: 2018.03.06,

https://www.nhm.ac.uk/discover/news/2018/march/explore-the-museum-with-sir-david-attenborough.html

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

Kevin Roose, The Latecomer's Guide to Crypto, What are DAOs? The New York Times, Technology, https://www.nytimes.com/interactive/2022/03/18/technology/what-are-daos.html

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/

Launch of the European Blockchain Regulatory Sandbox, 2023.02.14, https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox

Lauren Feiner, Lawmakers update Kids Online Safety Act to address potential harms, but fail to appease some activists, industry groups, CNBC, Tech, 2023.05.02., https://www.cnbc.com/2023/05/02/updated-kids-online-safety-act-aims-to-fix-unintended-consequences.html

Lego, Now some serious stuff, https://www.lego.com/en-us/kids/legal/privacy-policy-short

Marc Rotenberg, „Privacy in the Modern Age: The Search for Solutions", 38th International Conference of the Data Protection and Privacy Commissioners, Marrakech, 2016.10.19. Elérhető: https://archive.epic.org/privacy/intl/EPIC-38ICDPPC-kyn-10-16.pdf

Mattel Children's Privacy Statement, https://shop.mattel.com/pages/childrens-privacy-statement

Matt Sheehan, China's AI Regulations and How They Get Made, July 2023, https://carnegieendowment.org/files/202307-Sheehan_Chinese%20AI%20gov.pdf

Melissa Heikkilä, Our quick guide to the 6 ways we can regulate AI, MIT Technology Review, 2023.05.22, https://www.technologyreview.com/2023/05/22/1073482/our-quick-guide-to-the-6-ways-we-can-regulate-ai/

Mengting Xu, Lawsuit Challenges Constitutionality of California Age-Appropriate Design Code, California Lawyers Association, https://calawyers.org/privacy-law/lawsuit-challenges-constitutionality-of-california-age-appropriate-design-code/

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, 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

Meta, View and download your Meta account information, https://www.meta.com/en-gb/help/quest/articles/accounts/privacy-information-and-settings/view-your-information-and-download-your-information/

Microsoft Dynamics 365, What is augmented reality or AR?, https://dynamics.microsoft.com/en-gb/mixed-reality/guides/what-is-augmented-reality-ar/

Microsoft, Putting principles into Practice at Microsoft, https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimaryr5

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

Midjourney, https://www.midjourney.com/

Mike Wendling, QAnon: What is it and where did it come from? BBC News, 2021.01.06, https://www.bbc.com/news/53498434

National Artificial Intelligence Initiative, https://www.ai.gov/

Necz Dániel, Az adatkezelésről való tájékoztatás technológiai környezetben, különös tekintettel az Egyesült Államok szabályozására, Jogi Fórum, 2022, https://www.jogiforum.hu/wp-content/uploads/2022/09/necz-daniel_adatkezelesrol-valo-tajekoztatas-technologiai-kornyezetben_cimlappal.pdf

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, Business, 2019.06.07., https://www.wired.co.uk/article/china-social-credit-system-explained

Noor Nanji, Donald Trump to be allowed back on to Facebook and Instagram, BBC News, 2023.01.26, https://www.bbc.com/news/business-64408306

OECD, AI Principles, https://oecd.ai/en/ai-principles

OECD.AI, Japan, AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-25312

OECD.AI, Russian Federation, National Strategy for AI Development, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24901

Om Malik, Pokémon Go Will Make You Crave Augmented Reality, The New Yorker, Annals of Technology, 2016.07.12, https://www.newyorker.com/tech/annals-of-technology/pokemon-go-will-make-you-crave-augmented-reality

Open Letter to the European Commission, Artificial Intelligence and Robotics, https://www.politico.eu/wp-content/uploads/2018/04/RoboticsOpenLetter.pdf

Pause Giant AI Experiments: An Open Letter, https://futureoflife.org/open-letter/pause-giant-ai-experiments/

PCMag.com, Encyclopedia, Walled Garden, https://www.pcmag.com/encyclopedia/term/walled-garden

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/

Rockweel Anyoha: The History of Artificial Intelligence (Harvard SITN Blog): http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Rory Cellan-Jones, Stephen Hawking warns artificial intelligence could end mankind, BBC News, 2014.12.02, https://www.bbc.com/news/technology-30290540

Ryan O'Hare, Drones are being 'taught' to search for missing people: AI software works with quadcopters to explore forests and woods, https://www.dailymail.co.uk/sciencetech/article-3440694/Drones-taught-search-missing-people-AI-software-works-quadcopters-explore-forests-woods.html

Sam Thielman, Silk Road operator Ross Ulbricht sentenced to life in prison, https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

Siobhan Roberts, Christopher Strachey's Nineteen-Fifties Love Machine, 2017.02.14, https://www.newyorker.com/tech/annals-of-technology/christopher-stracheys-nineteen-fifties-love-machine

Strong AI vs. weak AI, IBM, https://www.ibm.com/topics/strong-ai

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

Virtual Reality in the Classroom, University of Toronto, Ontario Institute for Studies in Education, https://guides.library.utoronto.ca/c.php?g=607624&p=4938314

What is a chatbot? Oracle, https://www.oracle.com/ie/chatbots/what-is-a-chatbot/

What is generative AI? IBM, 2023.04.20, https://research.ibm.com/blog/what-is-generative-AI

Worker Info Exchange, Just Beat It! How Just Eat Robo-fires its Workers, 2023. április, https://www.workerinfoexchange.org/just-eat-report

Ződi Zsolt, A mesterséges intelligencia szabályozásának dilemmái. 1. rész: A mesterséges intelligencia (jogi) definíciója, https://www.ludovika.hu/blogok/itkiblog/2020/08/24/a-mesterseges-intelligencia-szabalyozasanak-dilemmai/ [2023.09.29.]

Jogszabályok jegyzéke:

Nemzetközi jogszabályok:

A 11., 14 és 15. Kiegészítő Jegyzőkönyv által módosított Emberi Jogok Európai Egyezménye, valamint az 1., 4., 6., 7., 12., 13. és 16. Kiegészítő Jegyzőkönyv, https://www.echr.coe.int/documents/d/echr/Convention_HUN

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

The Convention on the Rights of the Child: The child-friendly version, UNICEF https://www.unicef.org/sop/convention-rights-child-child-friendly-version

Európai uniós jogszabályok és egyéb dokumentumok:

Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, OJ L 281, 23.11.1995, p. 31–50 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), OJ L 201, 31.7.2002, p. 37–47 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)

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), OJ L 2, 4.1.2002, 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, OJ L 119, 4.5.2016, 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

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg), OJ L 119, 4.5.2016, p. 1–88 (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) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, OJ L 194, 19.7.2016, p. 1–30 (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 Rendelete, az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), Brüsszel, 2017.1.10. COM(2017) 10 final, 2017/0003(COD)

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 2019/2161 irányelve (2019. november 27.) a 93/13/EGK tanácsi irányelvnek, valamint a 98/6/EK, a 2005/29/EK és a 2011/83/EU európai parlamenti és tanácsi irányelvnek az uniós fogyasztóvédelmi szabályok hatékonyabb végrehajtása és korszerűsítése tekintetében történő módosításáról, PE/83/2019/REV/1, OJ L 328, 18.12.2019, p. 7–28 (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) 2019/1024 irányelve (2019. június 20.) a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83 (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) 2019/1024 irányelve a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83 (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, COM/2021/206 final

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, OJ L 360, 11.10.2021, 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, OJ L 360, 11.10.2021, 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)

Az Európai Parlament és a Tanács Rendelete a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról (adatmegosztási jogszabály), Brüsszel 2022.2.23. COM(2022) 68 final, 2022/0047(COD)

Az Európai Parlament és a Tanács (EU) 2022/868 rendelete (2022. május 30.) az európai adatkormányzásról és az (EU) 2018/1724 rendelet módosításáról (adatkormányzási rendelet), PE/85/2021/REV/1, OJ L 152, 3.6.2022, p. 1–44 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Javaslat, az EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE, a szerződésen kívüli polgári jogi felelősségre vonatkozó szabályoknak a mesterséges intelligenciához való hozzáigazításáról (a mesterséges intelligenciával kapcsolatos felelősségről szóló irányelv), Brüsszel, 2022.9.28, COM(2022) 496 final, 2022/0303(COD)

Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) 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, OJ L 265, 12.10.2022, 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). PE/30/2022/REV/1, OJ L 277, 27.10.2022, 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)

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg), PE/32/2022/REV/2, OJ L 333, 27.12.2022, p. 80–152 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

Javaslat, az Európai Parlament és a Tanács Rendelete, az (EU) 2016/679 rendelet végrehajtásával kapcsolatos további eljárási szabályok megállapításáról, Brüsszel, 2023.7.4., COM(2023) 348 final, 2023/0202(COD)

Európai Parlament, Jelentés - A9-0188/2023, 2023.05.22, COM(2021)0206

Amerikai jogszabályok:

AB 730, https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201920200AB730&version=20190AB73093CHP

Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/6580/text

An Act Preventing a Dystopian Work Environment (H.1873) törvény-tervezet, 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/billTextClient.xhtml?bill_id=201920200AB730

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

Children's Online Privacy Protection Act, https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter91&edition=prelim

California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Colorado Privacy Act, https://leg.colorado.gov/bills/sb21-190

Connecticut Personal Data Privacy and Online Monitoring Act, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022

Executive Order 13859 of February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

Gramm Leach Bliley Act, https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

H1063. sz. törvény-tervezet, https://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2023&sind=0&body=H&type=B&bn=1063

Health Insurance Portability and Accountability Act of 1996, https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

Indiana Consumer Data Protection Act, https://legiscan.com/IN/text/SB0005/id/2779850

Iowa Consumer Data Protection Act, https://www.legis.iowa.gov/legislation/BillBook?ga=90&ba=SF%20262

Kids Online Safety Act, https://www.congress.gov/bill/118th-congress/senate-bill/1409/text

Local Law 144 of 2021 regarding automated employment decision tools, https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page

Montana Consumer Data Protection Act, https://laws.leg.mt.gov/legprd/LAW0210W$BSIV.ActionQuery?P_BILL_NO1=384&P_BLTP_BILL_TYP_CD=SB&Z_ACTION=Find&P_SESS=20231

National Artificial Intelligence Act of 2020, https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210

Risch Leads Effort to Improve Small Businesses' Access to Cyber Security Resources, 2023.09.07, https://www.risch.senate.gov/public/index.cfm/pressreleases?ID=A39F60D7-657C-4B05-B707-D8FA31A05128

Senate Bill no. 362, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362

Tennessee Information Protection Act, https://legiscan.com/TN/text/HB1181/id/2672877

Texas Data Privacy and Security Act, https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/07/hb00004f.pdf?la=en&rev=d2ece1e4cc0c4a708453ab079b7f00f4&hash=22A797B43BCDE288DA18FEB244DAF1A7

The California Age-Appropriate Design Code Act, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

Utah Consumer Privacy Act, https://le.utah.gov/~2022/bills/static/SB0227.html

Virginia Consumer Data Protection Act, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

Magyar jogszabályok és egyéb dokumentumok:

A Polgári Törvénykönyvről szóló 2013. évi V. törvény

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

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

További országok jogszabályai és egyéb anyagok:

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

Freedom of Information Act 2000 (FOIA) Decision Notice, ICO, 2022.02.08, https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4019607/ic-80804-j7c6.pdf

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

OECD.AI, Pan-Canadian AI Strategy, https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-14828

Rome Call for AI Ethics, 2020.02.28, https://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rc_pont-acd_life_doc_20202228_rome-call-for-ai-ethics_en.pdf

Bírósági gyakorlat:

Emberi Jogok Európai Bíróságának gyakorlata:

Bărbulescu v. Románia 61496/08. sz. ügy

Az Európai Unió Bíróságának gyakorlata:

A Bíróság ítélete (nagytanács), 2022. augusztus 1-i, OT kontra Vyriausioji tarnybinės etikos komisija

A Törvényszék T-557/20. sz. ügyben hozott, 2023. április 26-i, Egységes Szanálási Testület v. európai adatvédelmi biztos ítélete 78. bekezdés

C-362/14. sz. ügyben hozott ún. Schrems I. ítélet

C-311/18. sz. ügyben hozott ún. Schrems II. ítélet

C-413/23 P. felülvizsgálati ügy

C-487/21. sz. ügyben hozott döntés

C-604/22. sz. ügyben előterjesztett előzetes döntéshozatali kérelem, https://curia.europa.eu/juris/showPdf.jsf?text=&docid=268123&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=1280722

Magyarországi gyakorlat:

28/2014. (IX. 29.) AB határozat

Kfv.II.37.243/2021/11.

További országok gyakorlata:

OLG Frankfurt am Main, Urteil vom 27.06.2019 - 6 U 6/19, https://openjur.de/u/2185336.html

Amerikai bírósági gyakorlat:

3:23-cv-3440. sz. ügy, keresetlevél (Alphabet, Google Deepmind, Google), https://fingfx.thomsonreuters.com/gfx/legaldocs/myvmodloqvr/GOOGLE%20AI%20LAWSUIT%20complaint.pdf

ACLU v. Clearview AI, https://www.aclu.org/cases/aclu-v-clearview-ai

OpenAI-al szemben benyújtott keresetlevél, Northern District of California, USA, https://clarksonlawfirm.com/wp-content/uploads/2023/06/0001.-2023.06.28-OpenAI-Complaint.pdf

Adatvédelmi hatóságok döntései, iránymutatások és egyéb hatósági anyagok:

Az Adatvédelmi Munkacsoport és az Európai Adatvédelmi Testület iránymutatásai és egyéb anyagok:

Adatvédelmi Munkacsoport 03/2014. sz. vélemény személyes adatok megsértése bejelentéséről, 693/14/EN, WP 213, elfogadva: 2014. március 25.

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.

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.

Az Adatvédelmi Munkacsoport automatizált döntéshozatallal és profilalkotással kapcsolatos wp251.rev.01 sz 2017. október 3-án meghozott, 2018. február 6-án felülvizsgált iránymutatása

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.

Az Európai Adatvédelmi Testület 4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 2.0 változat, elfogadás időpontja: 2020. október 20., 24.

European Data Protection Commission, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021.

Az Európai Adatvédelmi Testület 5/2020 Iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 1.1 verzió, elfogadás időpontja: 2020.05.04.

07/2020. sz. iránymutatás az Adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról

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

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, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 1.0, adopted on 22 May 2022.

Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland

Limited (Art. 65 GDPR)

A Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorlata:

NAIH/2019/55/5. 17.

NAIH/2019/1859. 11.

NAIH/2015/2201/17/H.

NAIH/2020/2729/15. 10.

NAIH/2020/1154/9. sz. határozat

NAIH-3151-2/2021. sz. határozata. 11.

NAIH-3975-1/2021. sz. ügyben hozott határozat

NAIH-85-3/2022.

NAIH-963-10/2022.

Francia adatvédelmi hatósági gyakorlat:

CNIL, Facial recognition: 20 million euros penalty against CLEARVIEW AI, 2022.10.20, https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

CNIL, Personalised advertising: CRITEO fined EUR 40 million, 22 June 2023, https://www.cnil.fr/en/personalised-advertising-criteo-fined-eur-40-million

Ír adatvédelmi hatósági gyakorlat:

Data Protection Commission announces €345 million fine of TikTok, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok#:~:text=The%20Data%20Protection%20Commission%20(DPC,TTL)%20on%201%20September%202023

Data Protection Commission, 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

Data Protection Commission, 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

Data Protection Commission, Subject Access Requests: A Data Controller's Guide, https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf

Data Protection Commission, Data Protection in the Workplace: Employer Guidance, April 2023, https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Data%20Protection%20in%20the%20Workplace%20Employer%20Guidance%20EN.pdf

Német adatvédelmi hatósági gyakorlat:

Baden Württemberg Adatvédelmi és Információszabadsági Biztosa („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

Berlin Adatvédelmi és Információszabadsági Biztosának („Berliner Beauftragte für Datenschutz und Informationsfreiheit") 2021. évi éves jelentése, https://www.datenschutz-berlin.de/infothek/publikationen/jahresberichte/

Berlin Adatvédelmi és Információszabadsági Biztosa, Computer sagt Nein, 2023.05.31, https://www.datenschutz-berlin.de/pressemitteilung/computer-sagt-nein/

Szászország Adatvédelmi és Információszabadsági Biztosának („Sächsische Datenschutz- und Transparenzbeauftragte") 2022. évi éves jelentése, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2022.pdf

Angol adatvédelmi hatósági gyakorlat:

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, 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

További adatvédelmi hatóságok gyakorlata:

A belga adatvédelmi hatóság 2022/21. sz. döntése, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf

Datatilsynet, Artificial intelligence and privacy, Report, January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362], 2022.03.09, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9751362

Garante per la protezione dei dati personali, Artificial intelligence: stop to ChatGPT by the Italian SA, Personal data is collected unlawfully, no age verification system is in place for children, 2023.03.31, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english

Hellenic Data Protection Authority, Imposition of fine on Clearview AI, Inc, 2022.07.13, https://www.dpa.gr/en/en/enimerwtiko/prakseisArxis/imposition-fine-clearview-ai-inc

Svéd adatvédelmi hatóság ("Swedish Authority for Privacy Protection"), Administrative fee against Spotify, megjelent: 2023.06.13, https://www.imy.se/en/news/administrative-fee-against-spotify/

További hatóságok döntései:

Gazdasági Versenyhivatal VJ/88/2016. sz. ügyben hozott határozata