NECZ DÁNIEL[19]

A MESTERSÉGES INTELLIGENCIA ADATVÉDELMI SZEMPONTJAI, KÜLÖNÖS TEKINTETTEL A BELÜGYI SZERVEK ADATKEZELÉSI GYAKORLATÁRA

Absztrakt

A mesterséges intelligencia (MI) egyre nagyobb hatással bír mindennapjainkra, ez pedig igaz a hatósági ügyintézésre vagy a bűnüldöző és nemzetbiztonsági szervek munkájára is. Ez utóbbi szervek esetén különösen kiemelt szempontot képez az MI alapú adatkezelés etikus, a lehetőségekhez mérten átlátható, valamint az érintettek jogait és szabadságait figyelembe vevő megszervezése, tekintettel az MI érintettek magánszférájával kapcsolatos kockázataira.

A fenti szempontoknak kell érvényesülnie például az egyes nyomozóhatóságok által alkalmazott kibervédelmi, valamint arcfelismeréssel járó és egyéb azonosításra szolgáló megoldások területén, amely utóbbiak tekintetében számos olyan szempont is felmerül, amelyek az adatkezelés sajátos megszervezését követelik meg. Így arcfelismerő rendszerek esetén különösen fontos a megfigyelt terület és az azzal kapcsolatos esetleges nemzetbiztonsági vagy más kockázatok (például: repülőterek megfigyelése), a megfigyelés időtartamának, valamint egyéb körülményeinek (például: az adott területen jellemző érintetti csoportok) figyelembevétele, és a rendszerek megfelelő és folyamatos felülvizsgálata.

Természetesen az MI alapú rendszerek rendvédelmi és nemzetbiztonsági célú alkalmazásuk mellett egyre jelentősebb szerephez jutnak az önkormányzati és egyéb hatósági ügyintézés támogatásában, ideértve különösen az állampolgárokkal történő kapcsolattartást segítő megoldásokat (például: chatbot és okos asszisztens megoldások), valamint a hatósági munkát segítő elemzőrendszereket.

Mint az a fentiekből is látható, a mesterséges intelligencia hatékonyan lehet képes a köz- és nemzetbiztonság támogatására, valamint a hatósági munkavégzés megkönnyítésére, azonban ez csakis az állampolgárok jogainak és szabadságainak megfelelő figyelembevételével foghat helyt.

Kulcsszavak: MI, arcfelismerés, biztonság, chatbot

[19] Pázmány Péter Katolikus Egyetem, Jog- és Államtudományi Kar, doktorandusz

THE DATA PROTECTION ASPECTS OF ARTIFICIAL INTELLIGENCE WITH SPECIAL FOCUS ON THE DATA PROCESSING PRACTICES OF ORGANS OVERSEEN BY THE HUNGARIAN MINISTRY OF INTERIOR

Abstract

The impact of artificial intelligence (AI) on our everyday life is growing day-by-day, which is true for the procedures of public administration, law enforcement and national security agencies as well. In case of these latter organs, the ethical and transparent usage of AI solutions with a focus on the rights and freedoms of the data subjects is of key importance with regard to the risks concerning the private sphere of the affected data subjects.

The above considerations must be taken into account, for example, concerning cybersecurity, facial recognition and other identification solutions used by law enforcement agencies, which require – especially in the latter cases – a number of special aspects concerning data processing operations. In line with the above, in case of facial recognition systems, it is particularly important to take into account the area being monitored and any related national security or other risks (such as risks concerning airports), the duration of monitoring and other circumstances (e.g. groups of data subjects related to the given area) and the appropriate and continuous revision of the systems.

Naturally, besides the use of AI solutions by law enforcement and national security agencies, AI is playing an increasingly important role in supporting municipalities and other authorities. This includes tools supporting communication with citizens (e.g. chatbots and smart assistant solutions) and systems supporting analysis of authorities.

With regard to the above, artificial intelligence can effectively support public and national security and facilitate the work of public administration, but only with regard to the rights and freedoms of citizens.

Keywords: AI, facial recognition, security, chatbot

1. Bevezetés

A mesterséges intelligencia korunk egyik legdinamikusabban fejlődő technológiája, amelyre sokan az áram vagy az internet feltalálása mellett az emberiség egyik legnagyobb teljesítményeként tekintenek, sokszor figyelmen kívül hagyva a technológiában rejlő lehetséges kockázatokat. Vitathatatlan tény azonban, hogy a technológia előnyei számos területen már napjainkban is megmutatkozni látszanak, ideértve például az arcfelismerési technológia bűnüldözési célú használatát, vagy a kereskedelmi szektorban és a közigazgatásban is egyre rapidabb módon elterjedni látszó chatbot alkalmazásokat. Mindemellett az MI alapú technológiáknak napjaink globalizációra és modern informatikai megoldásokra épülő cyberkultúrája is kedvező táptalajt nyújt, ahol az információhoz való hozzájutás szinte már alapszabadságnak tekinthető (*Perecz 2012: 22*).

A mesterséges intelligencia azonban számos előnye mellett értelemszerűen komoly kockázatokat is rejt magában, különösen ideértve a technológia sok esetben nehézkes kontrollálhatóságát és jellemzően nagy mennyiségű személyes adat kezelését. Így a térfigyelő kamerákhoz kapcsolódó különböző arcfelismerő rendszerek – bár jelentős bűnüldözési és közbiztonsági érdekek fűződnek kiterjedt alkalmazásukhoz –, az érintettek magánélete felett is fokozott ellenőrzéssel járhatnak, az alkalmazott rendszerek mögötti logika pedig sok esetben átláthatatlan marad az érintettek számára. Mindezen kockázatokat pedig csak növeli az MI adatéhsége, amely már az egyes rendszerek tesztidőszakában is megmutatkozik, ugyanis a mesterséges intelligencia fejlesztéséhez jellemzően adatok tömeges kezelésére van szükség. Így például több tízezer vagy akár több millió kép, szöveg vagy hangfelvétel elemzésére is szükség lehet ahhoz, hogy az adott algoritmus megbízható eredményeket adjon, és felmerülhessen „éles" alkalmazása, az általa gyűjtött adatok pedig csak az esetek egy részében anonimizálhatók, míg más esetekben már kifejezetten a kezdetektől fogva szükség van nagy mennyiségű személyes adat kezelésére. Így egy arcfelismerő programnak sok esetben már a tesztidőszakban is nagy mennyiségű emberi képmást kell beolvasnia ahhoz, hogy az emberi mimika, az egyes arcvonások és egyéb sajátosságok közötti különbségeket megtanulja, és felismerje, és képes legyen egy adott arcképet beláthatatlan számú egyéb arckép közül kellő bizonyossággal azonosítani. Mindemellett azonban egy chatbot alkalmazás adott esetben fiktív személyhez kapcsolódó szövegek beolvasásával is tesztelhető és fejleszthető addig a szintig, amíg nem szükséges egy konkrét személy azonosítása (például:

egy konkrét ügyfél azonosítása az érintett személy támogatásához, illetve a vele való kapcsolatfelvételhez).

Az adatvédelmi problémák, valamint ezzel összefüggésben a technológia és az automatizálás összefonódásából eredő dilemmák (*Gaszt 2019: 22*) kiküszöbölésére természetesen van ellenszer – ez pedig nem más, mint az átlátható, és a kezdetektől az adatvédelmi szabályok figyelembevételével megtervezett adatkezelés, amely a jogi és informatikai szempontok közös alkalmazását igényli. Fontos azonban leszögezni, hogy a megfelelő adatkezelés megtervezésekor minden egyes esetben figyelembe kell venni az adott rendszer vagy megoldás sajátosságait, az éles- és tesztalkalmazási időszakot, valamint a felhasznált adatkört. Csak ezek ismeretében dolgozható ki a megfelelő adatkezelési stratégia, a szükséges adatbiztonsági intézkedések köre, valamint szövegezhető meg az adatkezelés által érintetteknek szóló adatvédelmi tájékoztató és az adatkezelés jogszerűségének alátámasztásához szükséges esetleges további dokumentumok (például: a vonatkozó adatvédelmi hatásvizsgálat vagy az érdekmérlegelési tesztek dokumentációja).

Természetesen az MI általi adatkezelés problémája nem csak az adatkezelőkre hárul, hanem egyúttal egy olyan közös feladatnak is tekinthető, amely a teljes európai közösség és az egyes tagállamok számára is komoly kihívást jelent, ideértve mind az MI etikus használata keretrendszerének, mind a nemzeti és európai MI stratégiáknak a kialakítását és összehangolását.

A fentiekkel összhangban a jelen tanulmányomban össze kívánom foglalni a mesterséges intelligencia általi adatkezelés legfontosabb szempontjait, ideértve az adatkezelés megtervezését, a helyes jogalapok megválasztását, az érintetti jogok hatékony támogatását, valamint a megfelelő adatbiztonsági intézkedések alkalmazását. Mindemellett tanulmányomban kitérek a rendészeti, nemzetbiztonsági, valamint a Belügyminisztérium alárendeltségébe tartozó egyéb szervek adatkezelésének sajátosságaira, nemzetközi példákat is felvonultatva, valamint kiemelve az egyes, a gyakorlatban jelenlévő technológiák sajátosságait és a szükséges körben bemutatva az MI technológiai és informatikai hátterét.

2. A mesterséges intelligencia alapjai és etikai problémái

2.1. A mesterséges intelligencia meghatározása és története, a technológiával kapcsolatos etikai problémák

Az embert már a kezdetektől fogva foglalkoztatta a mesterséges intelligencia, és annak lehetősége, hogy a saját képére teremtsen magának segítőt (*Udvary 2018: 14*), azonban ennek képességével érthető módon még az utóbbi időkig nem rendelkezett. Ez azonban az emberi képzelőerőnek cseppet sem szabott gátat. A középkori és kora újkori alkimisták például úgy tartották, hogy az ember vagy legalábbis egy emberszerű, értelmes teremtmény (latin kifejezéssel homonculus, vagyis „emberke") mesterséges úton, akár egy kémcsőben is előállítható, a későbbi korok feltalálói pedig már kezdetleges, a mai robotokhoz hasonlítható gépezeteket is építettek. Erre jó példa Kempelen Farkas 18. századi, valójában vélhetőleg egy emberi kezelőt rejtő sakkozógépe, amely a 18. és 19. századi udvarokban és szalonokban jelentős népszerűségre tett szert.

Később az irodalom is egyre inkább érdeklődése középpontjába helyezte a gondolkodó gépeket. Erre jó példa az E.T.A Hoffmann Homokember című művében megjelenő, énekelni és beszélni is tudó női robot vagy a Karel Čapek nevű cseh drámaíró 1920-ban bemutatott, R.U.R. című darabja, amelynek a szláv nyelvekből eredeztetett „robot" szó mai értelmét is köszönhetjük (*Necz 2018: 53*). A fenti irodalmi előzmények nyomán néhány évtizeddel később határozta meg Isaac Asimov a robotika alapszabályait 1942-ben megjelent Körbe-körbe című novellájában[20]. Ezen három alaptörvénye vagy szabálya szerint:

- a robot nem tehet kárt emberben, és nem tűrheti, hogy az embert kár érje;
- a robot köteles engedelmeskedni az embernek, azonban ennek során nem szegheti meg a fenti első szabályt;
- a robot köteles magát megóvni, azonban ennek során nem sértheti meg a fenti két szabályt.

Az asimovi szabályok mellett a robotika és a mesterséges intelligencia etikai oldalát erősíti a 20. századi angol matematikusról elnevezett Turing-teszt is, amely a gépi értelem

[20]A mű eredeti angol nyelvű címe: „Runaround", amely elsőként az Astounding című amerikai folyóirat 1942. márciusi számában jelent meg.

emberi viselkedéshez való viszonyulását vizsgálja. A tesztet, vagy inkább játékot Turing 1950-ben publikált „Számítógép és értelem" című tanulmányában írja le, amelynek lényege, hogy a kérdező meg tudja-e állapítani beszélgetőpartneréről, hogy az ember-e vagy gép (számítógépes program) (*Turing 1950: 433*).

Természetesen a későbbi évtizedek nyomán sem lankadt az érdeklődés a mesterséges intelligencia iránt, amely a regények, majd tudományos magazinok lapjairól fokozatosan lépett át a valóságba. Ennek köszönhetően a század közepétől egészen napjainkig a mesterséges intelligencia szédítő fejlődést ért el[21], különböző megoldásokkal kísérletezve, hol intenzívebben, hol különböző akadályok miatt akadozva, mégis előre haladva (*Bőgel 2017: 2*), azonban ennek ellenére sem gyökerezett meg a témával kapcsolatos egységes definíciós készlet. Gyakorlatiasnak mondható meghatározást ad Magyarország Mesterséges Intelligencia Stratégiája, amely a mesterséges intelligenciát akként határozza meg, „*mint a betáplált adatok alapján önmagukat tanítani és javítani képes algoritmikus rendszerek összessége*[22]".

2.2. A mesterséges intelligencia alkalmazása a belügyi szervek gyakorlatában

Az MI alapú megoldások belügyi szervek gyakorlatában való rohamos elterjedése az egész világot érintő jelenség, a gyakran MI alapú megoldások alkalmazásával történő kibervédelmi feladatok ellátása, valamint ezen eszközök hatékony alkalmazása pedig a fenti szervek (ideértve különösen a bűnüldöző és nemzetbiztonsági szerveket) számára egyre inkább alapvető kötelezettségnek tekinthető (*Boda 2016: 126*). Különösen olyan területeken van helye az MI alapú technológiák alkalmazásának, ahol ez az emberi tevékenységet hatékonyan képes kiváltani, ideértve az adatgyűjtéssel, elemzéssel járó, valamint egyes szakértői feladatokat (*Miskolczi–Szathmáry 2018: 190-191*).

Természetesen azonban az MI alapú megoldások nem kizárólag a bűnüldöző és a nemzetbiztonsági szervek munkáját képesek hatékonyabbá tenni. Napjainkban ugyancsak aktuális kérdésnek minősülnek a különböző elektronikus személyazonosítási és ügyintézési,

[21] A Norvég Adatvédelmi Hatóság 2018. évi jelentése a mesterséges intelligenciáról és adatvédelemről (Artificial Intelligence and Privacy Report) („Norvég Adatvédelmi Hatóság Jelentése"), 6. Forrás: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [2020.11.15.]

[22] Magyarország Mesterséges Intelligencia Stratégiája 2020-2030, 2020. május („Magyarország MI Stratégiája"), 6. Forrás: https://digitalisjoletprogram.hu/files/6f/3b/6f3b96c7604fd36e436a96a3a01e0b05.pdf [2020.11.15.]

illetve elektronikus kormányzati szolgáltatások, amelyek megkönnyítik az érintettek napi ügyintézést, csökkentik a hivatali apparátusra nehezedő ügyterhet, valamint erősítik az állam és az állampolgárok közötti kapcsolatot (*Szabó, Székely–Simon 2008: 154*).

A fentiek körében érdemes megemlíteni, hogy a mesterséges intelligencia belügyi célú alkalmazásával Magyarország Mesterséges Intelligencia Stratégiája is foglalkozik, amely – többek között – a rendvédelmet szolgáló ellenőrzési rendszerek bevezetését, honvédelmi alkalmazások és fejlesztések keresztülvitelét, valamint katonai nemzetbiztonsági célú MI képességek fejlesztését is célul tűzi ki az elkövetkező néhány éven belül, e körbe értve rendelkezésre álló mesterséges intelligencia technológiák nyomozási folyamatokba való bevezetését, valamint a technológia aktív kibervédelmi alkalmazását is[23].

A belügyi szervek általi MI megoldások alkalmazásának adatvédelmi szempontjaira a tanulmány későbbi részeiben térek ki, azonban érdemes előre bocsátani, hogy a belügyi szervek, különösen a rendvédelmi és nemzetbiztonsági szervek által folytatott egyes adatkezelésekre e tekintetben többféle szabály is vonatkozhat, amelyek alkalmazása egymást kizárhatja, vagy épp kiegészítheti. A részben vagy egészben automatizált módon végzett adatkezelésekre, valamint azon nem automatizált adatkezelésekre, ahol az adatok valamely nyilvántartási rendszer részét képezik, általánosságban az Európai Parlament és a Tanács (EU) 2016/679. sz. Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) („**GDPR**”)[24] rendelkezései irányadók[25], míg a személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére – a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó, az Európai Parlament és a Tanács (EU) 2016/680 irányelvét (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

[23] Magyarország MI stratégiája, 52-53.

[24] Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016R0679 [2016] OJ L119/1

[25] GDPR 2. cikk (1) bek.

helyezéséről[26], átültető –, az információs önrendelkezési jogról és információszabadságról szóló 2011. évi CXII. törvényt kell alkalmazni[27], a személyes adatoknak a fenti körbe nem eső kezelésére pedig a GDPR és az Infotv. szakaszai vegyesen alkalmazandók[28]. Így például, amennyiben a rendőrség polgári jogi szerződései teljesítése során eljáró szerződéses kapcsolattartók adatait kezeli, úgy a GDPR, míg büntetőeljárás keretein belül való eljárása esetén az Infotv. rendelkezései lesznek irányadók.

A fentiekre tekintettel tehát megállapítható, hogy a rendvédelmi és nemzetbiztonsági szervek adatkezelései esetén az adatkezelés körülményeinek figyelembevételével tudjuk csak megállapítani, hogy melyik jogszabály is alkalmazandó a vonatkozó adatkezelésre, és milyen mértékben.

3. A mesterséges intelligenciával folytatott adatkezelés szempontjai

Az MI általi adatkezelés sok szempontból eltérést mutat az adatkezelés egyéb eseteitől, másrészt azonban ugyancsak alkalmazandók rá az adatkezelés alapelvei, az adatkezelők pedig kötelesek biztosítani az érintetti jogok gyakorlását (például: az adatokhoz való hozzáférés biztosítását vagy adott esetben azok törlését). Mindez azonban a gyakorlatban kettős követelményt állít az MI alapú technológiákat alkalmazó adatkezelők felé: egyrészt biztosítaniuk kell az ezen rendszerekhez kapcsolódó informatikai környezetet és a rendszerek hatékonyságát, másrészt a technológia adta lehetőségeket csak az adatvédelmi szabályok által előírt keretek között használhatják ki, figyelembe véve az érintettek érdekeit is. Ez a látszólagos korlátozás azonban egyfajta „versenyelőnyt” is jelent, hiszen az etikus és az adatvédelmi szabályoknak megfelelő MI technológiák alkalmazása és elterjedése széleskörű társadalmi támogatottsággal rendelkezik, valamint kellő mértékben átláthatóvá teszi az egyes rendszereket az érintettek számára, így oszlatva el a technológia megbízhatóságával kapcsolatos kétségeket és félelmeket.

[26] Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A32016L0680 [2016] OJ L119/89

[27] Infotv. 2. § (3) bek.; 3. § 10a-c.

[28] Infotv. 2. § (4) bek.

3.1. Az adatkezelés jogalapja és jogszerűsége

A fentebb írtakkal összhangban az adatkezelés alapelvei különös jelentőséggel bírnak az MI technológiák segítségével folytatott adatkezelés megfelelő kidolgozása kapcsán, tekintettel arra, hogy ezen megoldások nagyszámú személyes adat kezelésével sok esetben az érintettekre elemi hatású döntések meghozatalához vezethetnek. Minderre tekintettel az egyes adatkezelőknek az MI alapú megoldások kialakítása és a vonatkozó adatkezelési műveletek kidolgozása során különösen az alábbi szempontokat kell figyelembe venniük:

- **Jogszerűség, tisztességes eljárás és átláthatóság:** az adatkezelés jogszerűségének, tisztességességének, valamint átláthatóságának alapelve megköveteli, hogy a személyes adatok kezelését az adatkezelők tisztességesen, az érintettek számára átláthatóan végezzék[29]. Mindez azt is jelenti, hogy az adatkezelés nem irányulhat az állampolgárok titkos vagy átláthatatlan módon történő megfigyelésére, és olyan esetekben is, ahol az érintettek előzetes tájékoztatását a bűnüldözési vagy nemzetbiztonsági érdekek gátolják, az érintetteknek lehetőségük kell legyen arra, hogy az egyes hatóságok által folytatott adatkezeléseket – legalább utólagos módon – áttekinthessék[30];

- **Célhoz kötöttség:** a célhoz kötöttség elvéből következik, hogy az adatok gyűjtése csak meghatározott célból, és e céllal összeegyeztethető módon történhet, ideértve az adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további kezelését[31]. Így például nem sérti a célhoz kötött adatkezelés alapelvét, amennyiben a chatbot alkalmazás használata során gyűjtött személyes adatokat kutatási vagy statisztikai célokból (például: az ügyfélkiszolgálási képesség hatékonyságának fejlesztése) kezelik tovább, azonban az adatkezelőnek ezen további adatkezelést is átláthatóvá kell tennie az érintettek

[29] GDPR 5. cikk (1) a) pontja.

[30] Ideértve az érintettek szükséges későbbi tájékoztatását vagy a bizonyíték felülvizsgálatával kapcsolatos, büntetőeljárási jogszabályok által biztosított jogok gyakorlását.

[31] GDPR 5. cikk (1) b) pontja.

számára (ideértve annak az irányadó adatvédelmi tájékoztatóban való egyértelmű bemutatását is);

- **Adattakarékosság:** az adattakarékosság elvével összhangban az adatkezelésnek annak célja szempontjából minden esetben megfelelőnek és relevánsnak kell lennie, és kizárólag a szükséges mértékre kell korlátozódnia[32]. Mindez természetesen azt is jelenti, hogy az adatkezelőknek el kell kerülniük a konkrét cél nélküli készletező adatkezelést;

- **Pontosság:** az adatkezelésnek pontosnak és naprakésznek kell lennie, amely értelemszerűen azt is jelenti, hogy az adatkezelőnek szükség esetén törölnie vagy felül kell vizsgálnia a pontatlan személyes adatokat[33], azonban, amennyiben ezen intézkedés épp az adatkezelés célját hiúsítaná meg (például: arcképelemzés céljából az érintettek korábban készült fényképeinek felhasználása), úgy akár már pontatlanná vált adatok is megőrizhetők az adatkezelés céljának megfelelően;

- **Korlátozott tárolhatóság:** ezen alapelvvel összhangban az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatkezelés céljainak eléréséhez szükséges ideig teszi lehetővé (például: az adott kamerarendszerhez kapcsolódó szoftverbe épített automatikus törlési megoldás). Az adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további kezelése azonban ezen esetekben sem jár az alapelv sérelmével[34];

- **Integritás és bizalmas jelleg:** ezen elv értelmében az adatkezelést olyan módon kell végeznie az adatkezelőnek, hogy – az adatkezelés körülményeit is figyelembe vevő módon, egyedileg megválasztott – megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítsa a személyes adatok megfelelő

[32] GDPR 5. cikk (1) c) pontja.

[33] GDPR 5. cikk (1) d) pontja.

[34] GDPR 5. cikk (1) e) pontja.

biztonságát[35], mindezzel pedig a GDPR a megfelelő adatbiztonsági szint garantálást a jogszerű adatkezelés vezércsillagává teszi;

- **Elszámoltathatóság:** az elszámoltathatóság elve egyfajta esernyő-alapelv, amely megköveteli az adatkezelőtől, hogy az adatkezelése során a fenti valamennyi alapelvnek megfeleljen, és ehhez kapcsolódóan képesnek kell lennie ezen megfelelőség igazolására is[36]. Ezen alapelvből a gyakorlatban az adatkezelő számos kötelezettsége levezethető, így ennek megfelelően a jogos érdeken alapuló adatkezelések esetén az adatkezelő köteles érdekmérlegelési tesztet, az adatkezelési idő lejártával pedig a személyes adatok törlésével és a leselejtezéssel érintett adathordozók megsemmisítéséről jegyzőkönyvet készíteni, és azt a hatóság, valamint az érintettek kérésére bemutatni[37].

Az MI általi adatkezelés helyes jogalapja az adatkezelés céljának és körülményeinek figyelembevételével határozható meg. Így például, amennyiben MI alapú szoftverrel kerül sor viselkedésalapú marketingüzenetek és egyéb ajánlatok küldésére vagy az érintettek számára történő megjelenítésére, úgy az érintettek hozzájárulása lesz a releváns jogalap. Erre jó példa a Sky nevű brit televízió, amely az előfizetőinek az általuk korábban nézett műsorok alapján jelenít meg programajánlatokat (*Carey 2018*). Természetesen azonban adott esetben az érintettek hozzájárulása hiányában is alkalmazhatók MI alapú megoldások. Így egy arcfelismerő rendszerrel ellátott kamerarendszer – az irányadó jogszabályi környezet, valamint az adatkezelő tevékenysége tükrében – alapulhat az adatkezelő jogos érdekén, a közérdeken vagy közfeladat ellátásán, illetve az adatkezelőre irányadó kötelező jogi előíráson is.

Amennyiben hozzájáruláson alapuló adatkezelésről beszélünk, úgy ennek esetén elengedhetetlen, hogy az érintettől beszerzett hozzájárulás „tájékozott” legyen, vagyis az

[35] GDPR 5. cikk (1) f) pontja

[36] GDPR 5. cikk (2) bek.

[37] Lásd: Nemzeti Adatvédelmi és Információszabadság Hatóság („NAIH”) NAIH/2019/2450 ügyszám alatt hozott állásfoglalása a személyes adatok törlésével és adathordozók megsemmisítésével kapcsolatban, 3-4.

érintett az adatkezelésről, valamint jogai gyakorlásával kapcsolatban a hozzájárulás megadásához kellő információval rendelkezhessen, és azt erre tekintettel önkéntesen adhassa meg. E körben a hozzájáruló nyilatkozat megadható papíralapon vagy elektronikus formában is, a választott formának azonban igazodnia kell az adatkezelés sajátosságaihoz. Amennyiben például a hozzájárulást az adatkezelő egy kísérleti MI alkalmazáshoz kéri, amelyet zárt környezetben tesztel, úgy megfelelő lehet az érintettektől papíralapú hozzájáruló nyilatkozat bekérése, míg amennyiben az MI alkalmazást közösségi média platformok, weboldalak vagy alkalmazások használata során gyűjtött információk alapján történő marketing tartalmak generálásához használják fel, úgy helyesebb az érintett hozzájárulását elektronikus formában bekérni (például: az adott alkalmazáson belül megjelenő négyzet bepipálásával). Ilyen megoldásról beszélhetünk például a Google vagy egyéb böngészőprogramok vagy közösségi médiaszolgáltatók által használt adatalapú reklámszolgáltatások (ún. adtech szolgáltatások) esetén[38]. Jó megoldás továbbá, ha a hozzájáruló nyilatkozathoz az adatkezelő az adatkezelésről és az érintettek adatvédelmi jogairól és jogorvoslati lehetőségeiről részletes információkat nyújtó adatvédelmi tájékoztatót mellékeli (papíralapú nyilatkozat esetén például a tájékoztató papíralapú csatolásával, elektronikus úton bekért nyilatkozat esetén pedig közvetlenül az adatvédelmi tájékoztatóra mutató internetes hivatkozás megadásával). A nyilatkozatnak azonban ez esetben is tartalmaznia kell az érintettek tájékozott döntésének meghozatalához szükséges leginkább esszenciális információkat, ideértve az adatkezelő személyére, az adatkezelés céljára, a gyűjtött adatok körére, a hozzájárulás visszavonásához való jogra, az esetleges automatizált döntéshozatalra, illetve profilalkotásra, valamint a harmadik országba történő adattovábbításra vonatkozó információkat[39]. Ami a hozzájáruló nyilatkozat és a hozzá kapcsolódó tájékoztatás nyelvezetének megfogalmazását illeti, itt a kulcsot minden esetben a közérthetőség, illetve a világos és egyszerű nyelvezet képezi[40], amely azonban értelemszerűen mást jelent egy átlagfogyasztó, egy általános iskolás gyermek

[38] Lásd: az angol adatvédelmi hatóság adatalapú reklámszolgáltatásokkal kapcsolatos iránymutatása (Information Commissioner's Office (ICO) – Update report into adtech and real time bidding), 2019. június 20., 5-6. Elérhető: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/ [2020.11.15.]

[39] Az Európai Adatvédelmi Testület 2020. május 4. napján elfogadott, 05/2020. iránymutatása a hozzájárulásról, 1.1. verzió („05/2020 Iránymutatás"), 15-16. Lásd: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [2020.11.15.]., 13.

[40] GDPR (42) preambulum-bekezdés.

és egy elméleti kutató számára, amennyiben pedig az adatkezelés fogyatékossággal élő személyeket is jellemzően érint, úgy az adatkezelőnek törekednie kell arra, hogy az akadálymentesen megismerhető legyen ezen érintettek számára is (például: a weboldal programozása során lehetővé kell tennie a honlapot üzemeltető adatkezelőnek, hogy az ott elhelyezett adatvédelmi tájékoztatót, valamint a hozzájáruló nyilatkozat szövegét vakokat és gyengén látókat segítő szoftverek is be tudják olvasni)[41]. Amennyiben pedig az érintettek gyermekek (például: egy gyermekek képeit elemző algoritmus fejlesztése és tesztelése kapcsán), úgy az adatvédelmi tájékoztatót attól függetlenül is az adott korosztályba tartozó gyermekek számára érthető nyelven kell megfogalmaznia az adatkezelőnek, ha a hozzájárulást az adatkezeléshez a gyakorlatban nem maga a gyermek, hanem a nevében annak törvényes képviselője adja meg[42]. Általánosságban azonban leszögezhető, és valamennyi érintetti csoport esetén elvárható a túlzottan általános megfogalmazás (például: „marketing vagy üzletfejlesztési tevékenység folytatása”), valamint indokolatlan szakzsargon használat[43] kerülése. A fentieken túl a hozzájárulás visszavonását is éppoly egyszerű módon kell lehetővé tenni az érintett számára, mint a hozzájárulás megadását. Ez MI alapú megoldások esetén jelentheti a rendszer adott funkciójának elektronikus felületen való kikapcsolásának biztosítását[44]. Nem fogadható el azonban, ha az adatkezelő az érintettől például költségek megtérítését kéri a hozzájárulás visszavonásáért, vagy egyéb olyan hátrányokat érvényesít, amelyeket az egyébként a hozzájárulás alapján folytatott adatkezelés megszüntetése nem indokol[45].

Természetesen a hozzájáruláson alapuló adatkezelés mellett a gyakorlatban számos egyéb jogalap is szóba jöhet az MI alapú adatkezeléseknél, ideértve akár a szerződés teljesítését vagy a szerződés megkötését megelőzően az érintett kérésére történő lépések

[41] A NAIH ajánlása az előzetes tájékoztatás adatvédelmi követelményéről, 5, 18.

[42] Gyermekeknek szóló adatvédelmi tájékoztatáshoz példaként használható az ENSZ Gyermek Jogairól szóló Egyezmény gyermeknyelven írt szövege. Forrás: https://www.unicef.org/sop/convention-rights-child-child-friendly-version [2020.11.15.]

[43] A NAIH előzetes tájékoztatás adatvédelmi követelményéről szóló ajánlása például ilyen, az érintettek számára nem közismert szakzsargonnak tekinti a „targetálás” kifejezés használatát is (bővebben lásd: az ajánlás 8-9. oldalán lévő magyarázat)

[44] Norvég Adatvédelmi Hatóság Jelentése, 28.

[45] 05/2020 Iránymutatás, 13.

megtételét is. Tekintettel azonban arra, hogy kifejezetten MI alapú megoldások alkalmazására irányuló – közvetlenül az érintettekkel kötött – szerződések a gyakorlatban még ritkább esetben fordulnak elő, így ezekkel egyelőre még kevéssé találkozhatunk, ahogyan – kifejezetten MI alapú megoldások alkalmazását előíró jogi kötelezettség híján – az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez használt megoldásokkal is. Az ilyen előírások megjelenése a jövőben várhatóan fokozottan érinti majd például a közlekedés területét, tekintettel arra, hogy egyre több közlekedési eszköz rendelkezik MI alapú technológiát alkalmazó biztonsági rendszerekkel, amely adott esetben személyes adatok kezelését is végzi (például: gyalogosok felismerése a balesetek megelőzése céljából). Ami az érintett vagy más személyek létfontosságú érdekeinek védelme céljából folytatott adatkezeléseket illeti, itt egyelőre szintén kevés MI alapú technológiával találkozhatunk, azonban már napjainkban is akadnak olyan megoldások, amelyek mesterséges intelligenciával segítik mentési munkálatok folytatását. Erre jó példának tekinthető a Zürichi Egyetem, az MI kutatásokkal foglalkozó Dalle Molle Intézet, valamint az NCCR Robotics nevű társaság által fejlesztett, drónokba építhető szoftver, amely képes az emberi nyomok (például: eltévedt túrázók) felderítésére (*Nichols 2016*). Mindemellett közérdekű vagy az adatkezelőre ruházott közhatalmi feladatok gyakorlása, továbbá az adatkezelő jogos érdeke is alapul szolgálhat az MI megoldások útján történő adatkezeléshez, különösen térfigyelő kamerákkal vagy biztonsági célból alkalmazott egyéb rendszerekkel összefüggésben. Az első esetben hangsúlyozandó azonban, hogy az ezen jogalapra hivatkozó adatkezelőnek közhatalmi vagy egyéb, közfeladatot ellátó szervnek kell lennie (ideértve akár közfeladatot ellátó gazdasági társaságokat vagy civil szervezeteket is)[46], amelyet közvetlenül jogszabály vagy erre jogosultsággal rendelkező szerv jelöl ki. Mindezt megerősíti a NAIH közterületi térfigyelő kamerák üzemeltetésével járó adatkezeléssel kapcsolatos állásfoglalása[47] is, amely hangsúlyozta, hogy ilyen, illetve ehhez kapcsolódó adatkezelést jogszerűen csak az arra jogszabályi felhatalmazással rendelkező rendőrség[48], valamint közterület-felügyelet[49], illetve

[46] GDPR (80) preambulum-bekezdés.

[47] NAIH/2015/6921/2/V. ügyiratszámú NAIH állásfoglalás.

[48] Lásd: a Rendőrségről szóló 1994. évi XXXIV. törvény 42. § (1) bek.

[49] Lásd: a közterület-felügyeletről szóló 1999. évi LXIII. törvény 7. § (2)-(4) bekezdései.

szintén meghatározott körben a jogszabályban megjelölt egyéb szerv[50] alkalmazhat. Saját területen azonban például arcfelismerő rendszerrel vagy egyéb hasonló MI alapú technológiával ellátott biztonsági kamerarendszert közhatalmi, vagy egyéb közfeladatot ellátó szerveken túl egyéb személyek is alkalmazhatnak, az ehhez fűződő jogos érdeküket azonban összefoglaló módon fel kell tüntetniük a vonatkozó adatvédelmi tájékoztatójukban, valamint részletesen ki kell fejteniük a jogos érdeküket alátámasztó érdekmérlegelési tesztben. Ezen dokumentumban az adatkezelőnek meg kell határoznia az adatkezelés alapjául szolgáló jogos érdekét, az annak ellenpólusát képező érintetti érdeket, és az adatkezelés egyéb körülményeire is figyelemmel meg kell állapítania az érdekmérlegelési teszt eredményét – miszerint kezelhető-e egyáltalán a vonatkozó személyes adat[51]. Ezzel kapcsolatban hangsúlyozandó, hogy a teljes érdekmérlegelési tesztet az adatkezelő nem köteles az érintett részére előzetesen bemutatni vagy egyéb módon nyilvánosságra hozni (például: a saját honlapon), azonban – kérésre – azt az érintett vagy az adatvédelmi hatóság részére be kell mutatnia. Hangsúlyozandó azonban, hogy a fentiektől eltérően az adatkezelő dönthet úgy is, hogy az érintetti jogok támogatása érdekében nyilvánosságra hozza az adatkezeléshez kapcsolódó érdekmérlegelési tesztet[52].

A fentieken túl hangsúlyozandó, hogy amennyiben a személyes adatok különleges kategóriáinak[53] kezelésére kerül sor, úgy a GDPR 6. cikke szerinti megfelelő jogalapra történő hivatkozás mellett az adatkezelőnek a GDPR 9. cikke szerinti, a különleges adatokra irányadó releváns feltételt is igazolnia kell. Ilyen feltétel lehet például egy pert megelőző szöveges bizonyítékok után kutató szoftver alkalmazása (*Ződi 2018: 8*) esetén a jogi igények előterjesztésének, érvényesítésének, illetve védelmének[54], míg egy egészségügyi adatokat gyógyszerkutatási szempontból elemző szoftver esetén például a népegészségügyi területet érintő közérdek szükségessége[55]. Az egészségügyi adatok kapcsán hangsúlyozandó azonban,

[50] Lásd: a NAIH/2020/4103. ügyszám alatt hozott adatvédelmi állásfoglalás, 3.

[51] Lásd: a NAIH előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlása, 12.

[52] Erre a gyakorlatban jó példa a MOL Nyrt. chatbot alkalmazással kapcsolatos érdekmérlegelési tesztje. Lásd: https://mol.hu/images/mol_hu/pdf/others/mol_chatbot/MOL-chatbot-adatveedelmi-tajekoztato.pdf [2020.11.15.]

[53]Ideértve a GDPR 9. cikk (1) bekezdésével összhangban például az érintettek egészségügyi, biometrikus vagy genetikai adatait.

[54] GDPR 9. cikk (2) f) pontja.

[55] GDPR 9. cikk (2) i) pontja.

hogy az e vonatkozásban irányadó külön szabályozási rezsim mellett a vonatkozó orvosetikai kérdések is különös hangsúlyt élveznek. Így az elkövetkezendő években adatvédelmi szempontból kihívást jelent majd a funkciójukat vesztő, sérült emberi szervek vagy testrészek okos-protézisekkel vagy hasonló rendszerekkel történő pótlása is (például: ezen rendszerek memóriájának feltöltése és törlése) (*Klein 2018: 211*).

3.2. Az érintetti jogok gyakorlása

Az érintetti jogok gyakorlása az MI alapú adatkezelések esetén kiemelt hatással bír, tekintettel arra, hogy az egyes MI alapú megoldások az érintettek olyan szokásait is képesek feltérképezni, amelyek a magánéletük inherens részét képezik, az azokkal kapcsolatos műveletek végzése pedig sok esetben önmagában túlmutathat az adatkezelés célja által indokolt mértéken.

A tájékoztatás kapcsán az általunk fentebb írtak tekintendők irányadónak. Erre tekintettel tehát az adatkezelőnek szükséges világosan és közérthetően az érintettek tudomására hoznia az adatkezelés főbb jellemzőit, ideértve különösen az adatkezelés célját, jogalapját, a kezelt adatok körét, az adatkezelés időtartamát, és az esetleges adattovábbítások címzettjeit[56]. Az érintettek tájékoztatása tekintetében még szigorúbb követelményeket támaszt a GDPR az adatkezelőkkel szemben, amennyiben automatizált döntéshozatalra[57], illetve profilalkotásra[58] is sor kerül. Így tehát, amennyiben az adatkezelő emberi beavatkozás nélkül folytat online munkaerő-toborzási tevékenységet bizonyos pályázók vonatkozásában[59], úgy az automatizált döntéshozatal tényén túl köteles tájékoztatni az érintetteket legalább az alkalmazott logikára és arra vonatkozó információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír[60]. Mindezt pedig

[56] Lásd: GDPR 13-14. cikkei.

[57] Ideértve a GDPR 22. cikk (1) bekezdése értelmében a kizárólag automatizált adatkezelésen alapuló olyan döntéseket, amelyek esetén a döntés hatálya az érintettre nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

[58] A GDPR 4. cikk 4. pontja szerint ide tartozik a személyes adatok kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos jellemzők értékelésére használják.

[59] GDPR (71) preambulum-bekezdés.

[60] GDPR 13. cikk (2) f) pontja, 14. cikk (2) g) pontja.

értelemszerűen az adatkezelőnek – hacsak nem kizárólag informatikai szakértőkből áll az érintetti kör – a technikai szakzsargont nélkülözve, közérthetően kell megtennie, ami az MI alapú alkalmazások területén azért is kiemelten nehéz feladat, mert a rendszer egyes működési elvei és a mögöttük lévő logika megfejtése sokszor még a szakértők számára sem teljesen világos[61].

A tájékoztatáson túl ugyancsak kulcsfontosságúnak minősül a hozzáférési jog gyakorlása, amely lehetővé teszi az érintett számára az adatkezelés jogszerű folytatásának ellenőrzését[62], továbbá az adatkezelő által kezelt személyes adatairól (ideértve például: biztonsági kamerák által kezelt felvételeket vagy a chatboton keresztüli üzenetváltást) történő másolatkérést. A másolat kiadása tekintetében azonban az adatkezelőnek számos szempontra kell figyelemmel lennie, ideértve különösen a másolatok formáját, a másolat által érintett személyes adatok körét, és a kapcsolódó költségeket. A másolat formája tekintetében elsődlegesen az érintett által meghatározott forma irányadó az ésszerűség és a technikai lehetőségek figyelembevételével. Például: egy hangfelvétel esetén az érintett kérheti a másolat e-mail csatolmányként vagy CD, illetve DVD lemezen történő kiadását is, de egy adatkezelő által szolgáltatandó teljes merevlemez kiadására irányuló kérelmet az adatkezelő jellemzően már nem köteles teljesíteni. Amennyiben az érintett a másolat kiadására irányuló kérelmet elektronikus formátumban nyújtotta be, és a másolat egyéb módon (pl. papíralapon) történő kiadását nem kérte, úgy a másolatot az adatkezelőnek széles körben használt, elektronikus formátumban[63] kell rendelkezésre bocsátania (ideértve például hangfelvételek esetén az elterjedtnek számító mp3 formátumot, dokumentumok esetén pedig a PDF formátumot).

Amennyiben az érintett a közelmúltban már kért másolatot az adatkezelőtől az érintett adatok vonatkozásában, és az újabb másolatkérést egyéb körülmény nem indokolja (például: az adatok időközben történt helyesbítése vagy adatkezelő általi módosítása), úgy ezen további másolatokért az adatkezelő adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel[64]. Hangsúlyozandó, hogy jelenleg nincs olyan jogszabály vagy egyértelmű adatvédelmi hatósági gyakorlat, amely az ilyen díjtételekre minimum- vagy

[61] Ezt nevezik a gyakorlatban ún. „fekete doboz” problémának is.

[62] GDPR (63) preambulum-bekezdés.

[63] GDPR 15. cikk (3) bek.

[64] Uo.

maximumtételeket rögzítene, az azonban leszögezhető, hogy az adatkezelő által megállapított díjtételeknek a másolat előállításához szükséges költségeknek kell megfelelniük, attól nem rugaszkodhatnak el, és így nem irányulhatnak az érintettek másolatkérési jogának gyakorlásától való eltántorítására. Amennyiben azonban a hozzáférési jog – vagy akár egyéb érintetti jog – gyakorlása által az érintett valós célja kifejezetten az adatkezelő eljárásának zavarása vagy az ügyintézővel szembeni személyes elégtétel[65], úgy a kérelem teljesítése kapcsán az adatkezelő ésszerű mértékű díjat számíthat fel, vagy akár meg is tagadhatja az érintetti kérelem teljesítését[66]. Amennyiben azonban az érintett a másolatok kiadását kizárólag elektronikus formátumban kéri, és ennek elkészítése az adatkezelő által könnyen, költségtételek felmerülése nélkül elvégezhető, úgy értelemszerűen az első kérelmet követő további másolatkérések esetén sem számolhat fel díjat az adatkezelő (például: a rendszer automatikusan, néhány percen belül képes elérhetővé tenni az érintettről kezelt adatokat)[67].

A másolatkéréshez való jog, bár a fentiekre tekintettel széleskörű lehetőségeket biztosít az érintett számára az adatkezelés jogszerűségének ellenőrzésére[68], azonban nem érintheti hátrányosan mások jogait és szabadságait, valamint annak teljesítése kapcsán az adatkezelő saját érdekei védelmét is figyelembe veheti (például: üzleti titok vagy szellemi tulajdon védelme). Ez azonban az adatkezelő számára azt a követelményt is támasztja, hogy olyan esetekben, ahol az érintett által kért másolat egyéb személyek adatait is tartalmazhatja (például: kamerafelvételek), ott mérlegelnie kell, hogy a másolat kiadása hátránnyal járhat-e ezen egyéb személyek részére, és amennyiben igen, úgy ez a hátrány milyen mértékű. Ugyanezen kötelezettség hárul az adatkezelőre azon esetben is, ha az érintett csak adatai megtekintését kívánja (például: felvételek meghallgatása vagy visszanézése, dokumentumok helyszínen történő elolvasása), azonban ilyen esetekben az érintettekre gyakorolt hatás eltérő mértékű lehet. Kamerafelvételek esetében például a felvételek megtekintésének biztosítása

[65] Lásd: az ICO egyértelműen megalapozatlan vagy túlzó kérelmekkel kapcsolatos tájékoztatása. Elérhető: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/ [2020.11.15.]

[66] GDPR 12. cikk (5) bek.

[67] Hasonlóan, jellemzően igen rövid idő alatt képes a Facebook nevű közösségi médiaoldal összesíteni a felhasználókról gyűjtött adatokat, és azokat az érintettek számára letölthetővé tenni (lásd: https://hu-hu.facebook.com/help/212802592074644) [2020.11.15.]

[68] GDPR (63) preambulum-bekezdés.

kisebb mértékben korlátozza a felvételen szereplő egyéb érintettek személyes adatok védelméhez fűződő jogát, mint a másolat kiadása, különösen, ha az érintett ezen személyekkel a felvételkészítés helyszínén találkozott (például: ugyanazon időpontban voltak jelen az adott helyszínen ügyintézés céljából)[69]. Amennyiben a másolat kiadása tekintetében azonban az adatkezelő mégis úgy ítéli meg, hogy az az azon szereplő egyéb érintettek jogaira sérelmes lehet, úgy a kérelem megtagadása helyett lehetőség szerint az adott felvétel egyéb érintettekre vonatkozó részét anonimizálnia kell (pl. az érintett részek kitakarásával), és csak az ezzel nem érintett részt kell a másolatot igénylő érintett részére kiadnia[70]. Hasonló megoldással élhet az adatkezelő az üzleti titoknak minősülő vagy szellemi tulajdonjog által védett információi esetén is. Szélsőséges esetben ezen egyéb érintetti vagy adatkezelői érdekek védelme a másolatkiadás megtagadásához is vezethet, ez azonban csak végső lehetőség az adatkezelő számára, ha a kérelem teljesítésére egyéb úton nincs mód (például: az érintett a biztonsági kamera felvételein túl az arcfelismerő szoftverhez használt forráskód kiadását is kéri, amely esetben ezen utóbbi kérelem tagadható meg). Hangsúlyozandó továbbá, hogy az érintett hozzáférési kérelmének teljesítése másolat kiadása esetén sem vezethet új adatok előállításához vagy a személyes adatokon az adatkezelő általi további műveletek végzéséhez. Így például: a kamerafelvételek kiadása mellett az érintett – hacsak az adatkezelő ilyen listával eleve nem rendelkezik – nem kérheti az adatkezelő által kiadott felvételek külön mellékletben történő felsorolását vagy rendszerezését[71].

A fentieken túl a gyakorlatban az egyéb érintetti jogok teljesítése is sajátosan érvényesül az MI általi adatkezelés területén, ideértve például a helyesbítéshez fűződő jogot. Ezen jog keretében az érintett a rá vonatkozó pontatlan személyes adatok helyesbítését, vagy – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is kérheti, azonban csak az adatkezelés technikai korlátjaira figyelemmel.

Ami az elfeledtetéshez, és így az adatok törléséhez való jogot illeti, az érintettet MI alapú adatkezelések esetén is jogosult ezen jog gyakorlására. Így például kérheti viselkedésalapú marketinghez adott hozzájárulása alapján kezelt viselkedési adatai törlését (például: helymeghatározási adatai törlése az általa rendszeresen látogatott helyiségek,

[69] NAIH/2019/1859 ügyszám alatt hozott határozata, 11.

[70] Uo.

[71] Uo.; 12.

szokásai kapcsán). Nem kérheti azonban például – az ezen jog vonatkozásában a GDPR 17. cikk (3) bekezdés szerinti kivétel-szabályokkal összhangban – a kizárólag kutatási célú MI rendszerek által kezelt adatai, valamint közhatalmi jog gyakorlása vagy jogi kötelezettség teljesítése érdekében kezelt adatai törlését. Ennek értelmében az arcfelismerő technológiával azonosított elkövető sem kérheti az eljáró hatóságtól vagy bíróságtól a térfigyelő kamera által róla készített felvételek törlését, ha a felvétel rögzítése és felhasználása egyébként jogszerűen történt.

Az MI alapú technológiák sajátosságain túl sok esetben kérdésesen érvényesülhet az adatkezelés korlátozásához, valamint az adathordozhatósághoz fűződő jogok gyakorlása is. Az első esetben az adatok érintett kérelmére történő korlátozása esetén az adatkezelőtől elvárható, hogy az adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből kezelje[72]. Mindez azt is jelenti, hogy az adatkezelőnek a rendelkezésére álló lehetőségek keretei között el kell különítenie a zárolt adatokat az egyéb, „aktív" adatoktól (például: egy publikus internetről is részben elérhető adatbázisból egy másik, zártan kezelt, valamint szűkebb körű hozzáférést engedő rendszerre kell azokat áthelyeznie), azonban ezen jog már nem feltétlenül érvényesülhet valamennyi MI alapú megoldás esetén, ha az alapul fekvő adatok zárolása – azok milyensége vagy mennyisége okán – a rendszer működését jelentősen korlátozná vagy veszélyeztetné. Ilyen esetekben adott esetben elfogadható lehet, ha az adatkezelő az érintett kérelmét csak később teljesíti. Ami pedig az adathordozhatósághoz való jogot illeti, itt mind az érintett adatok tagolt, széles körben használt, géppel olvasható formátumban való rendelkezésre bocsátásának, mind az adatok más adatkezelők részére történő továbbításának teljesítése[73] kérdéses lehet, ezen esetekben ugyanis épp az MI rendszer informatikai környezete és sajátosságai akadályozhatják meg a kérelem teljesítését. Hasonló problémát jelenthet, például, ha egy olyan versenytárs részére kéri továbbítani az érintett az adatkezelő saját rendszerében tárolt adatait, amely ezek olvasásának képességével nem rendelkezik, vagy azzal csak az adatkezelő üzleti titoknak és szellemi tulajdonjog által védett információinak (például: a vonatkozó forráskódok) átadásával rendelkezne. Ilyen esetekben

[72] GDPR 18. cikk (2) bek.

[73] GDPR 20. cikk (1) bek.

megtagadható az érintetti kérelem teljesítése, azonban ezen lehetőséggel az adatkezelő csak végszükség esetén élhet, és lehetőség szerint legalább részben teljesítenie kell az érintetti kérelmeket. Nem foghat helyt például az érintett kérelmének megtagadása, ha az érintett egy hangelemző szoftver által feldolgozott és tárolt hangfelvétel kiadását kéri, amennyiben ez az adatkezelő által technikai szempontból könnyen teljesíthető.

A fentebb írtakkal összhangban a személyes adatok MI alapú megoldásokkal közérdekből vagy közfeladat ellátása céljából, illetve az érintett jogos érdeke alapján történő kezelése – különösen a rendvédelem területén – főként biztonsági célú, valamint a közbiztonság garantálására és más személyek életének, testi épségének védelmére irányuló adatkezelések esetén foghat helyt. Az ilyen adatkezelések ellen azonban az érintett jogosult lehet tiltakozni, amely esetekben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, 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[74]. A közvetlen üzletszerzés érdekében folytatott adatkezelést azonban az adatkezelőnek tiltakozás esetén feltétlenül meg kell szüntetnie[75], így a viselkedésalapú marketing esetén kezelt adatok tekintetében nem érvelhet azzal az adatkezelő, hogy azok esetén az adatkezelői érdekek elsőbbséget élveznének az érintett érdekeivel szemben.

Amennyiben tehát az adatkezelő jogos érdeke alapján kezel személyes adatokat (ideértve például: az adott területen arcfelismerő rendszerrel ellátott kamerarendszer telepítését), úgy ezen megoldás alkalmazásának szükségességét az érdekmérlegelési tesztben kell bemutatnia, amelyben a fentebb ismertetetteken túl részletezendő

- az adott megoldás leírása és az ezzel kapcsolatos adatkezelés szükségességének ismertetése (például: az adott létesítmény védelme megköveteli arcfelismerő rendszer alkalmazását), valamint – ha ennek meghatározása szintén az adatkezelő jogos érdekén alapul – az adatmegőrzési idő meghatározásának szempontjai (például: a jogsértés észleléséhez, jogi igényérvényesítéshez szükséges időtartam)[76];

[74] GDPR 21. cikk (1) bek.

[75] GDPR 21. cikk (3) bek.

[76] Az Európai Adatvédelmi Testület 2019. július 10-én elfogadott, 3/2019. sz. iránymutatása a videókamerák segítségével történő adatkezelésekről, 24. Elérhető:

- korábbi példák, statisztikai kimutatás megadása, amelyek alátámasztják az adott rendszer alkalmazását az adatkezelésnél (például: az adott területet érintő magas bűnözési ráta)[77];
- az érintett jogainak korlátozása, az arra gyakorolt esetleges kockázatok, a fentiek mértéke[78].

A fenti információk segítségével tehát – az érdekmérlegelési teszt kérelmükre történő bemutatása esetén – az adatvédelmi hatóság és az érintett is felmérheti a jogos érdeken alapuló adatkezeléssel kapcsolatban az érintett jogainak korlátozását, az érintetti jogokra járó kockázatokat, illetve azok mértékét.

Ami az automatizált döntéshozatalt, illetve profilalkotást illeti, itt az adatkezelő fentiek szerint írt többlet-tájékoztatási kötelezettségén túl az érintetteket is bizonyos többlet-jogok illetik meg, amennyiben az ilyen módon történő adatkezelés

- kizárólag automatizált adatkezelésen alapul;
- az érintettre nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené[79].

Az első feltétel fennállásához azon körülményt szükséges megvizsgálnunk, hogy a döntéshozatal kizárólag automatizált adatkezelésen alapul-e. Amennyiben ugyanis az online hitelbírálat tekintetében a döntést teljes mértékben az algoritmus hozza meg, úgy ezen feltétel fennáll, amennyiben azonban a végső döntést egy emberi ügyintéző hozza meg, amelyet az algoritmus pusztán támogat (például: bizonyos számítások elvégzésével vagy adatbázisokból történő lekérdezéssel), úgy az adatkezelés nem kizárólag automatizált módon történik[80]. Amennyiben az első feltétel fennáll, úgy a második feltételt kell megvizsgálnunk, tehát, hogy a kizárólag automatizált módon végzett adatkezelés az érintettre nézve joghatással vagy

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [2020.11.15.]

[77] Uo., 8-9.

[78] NAIH/2019/55/5. ügyszám alatt hozott határozata, 17.

[79] GDPR 22. cikk (1) bek.

[80] Az Adatvédelmi Munkacsoport 2017. október 3-án elfogadott és 2018. február 6-án felülvizsgált, WP251rev.01 sz. iránymutatása az automatizált döntéshozatalról és a profilalkotásról, 9. Elérhető: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826 [2020.11.15.]

hasonlóan jelentős hatással jár-e. Az adatvédelmi hatósági gyakorlat szerint ezen kontextusban joghatással járónak minősülhet például a szerződés létrehozataláról vagy megszüntetéséről, szociális juttatás megadásáról vagy megvonásáról szóló döntés, míg hasonlóan jelentős hatásnak minősülhet a pénzügyi, egészségügyi, oktatási szolgáltatásokhoz való hozzájutással kapcsolatos, illetve adott esetben az érintettekre diszkriminatív módon ható döntés[81].

Olyan esetekben, amennyiben a fenti feltételek fennállnak, az adatkezelés kizárólag szerződés teljesítésén, az érintett hozzájárulásán, továbbá uniós vagy tagállami jog felhatalmazásán, ún. különleges adatok (pl. egészségügyi adatok) kezelése esetén pedig kizárólag az érintett kifejezett hozzájárulásán vagy közérdek szükségességén alapulhat[82]. Így tehát például az adatkezelő társaság az érintettek applikáción keresztüli vásárlási szokásainak elemzésével nem küldhet az érintettek részére saját jogos érdeke alapján direkt marketing üzeneteket, ahhoz ugyanis szükséges a hozzájárulásukat előzetesen beszereznie. Emellett, ha fenti valamelyik jogalapon meg is áll az adatkezelés, úgy az érintett jogosult arra, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be[83].

3.3. Az adatkezelés megszervezésének egyéb szempontjai

A fentieken túl a mesterséges intelligencia megoldások segítségével történő adatkezelések megszervezésének számos egyéb olyan szempontja lehet, amely akár külön tanulmányt is érdemelhetne, ideértve az adattovábbítási lehetőségeket, az adatkezelők és adatfeldolgozók közötti szerződéses kapcsolatok természetét, valamint az egyes informatikai megoldások adatvédelmi leképezését (például: az adatok tisztítását, különböző rendszerek felépítését stb.). Tekintettel a tanulmány terjedelmi kereteire, ezek közül pusztán néhány fontosabb szempontot emelnék ki, amelyek rávilágítanak arra, hogy az MI megoldásokkal történő adatkezelés megszervezése esetén milyen komplikált feladat is hárul az adatkezelőkre.

A fentiekre tekintettel kulcskérdésnek tekintendő az MI alapú adatkezelésekben közreműködő adatkezelők és adatfeldolgozók kapcsolatának szabályozása. E körben

[81] Uo., 21-22.

[82] GDPR 22. cikk (4) bek.

[83] GDPR 22. cikk (3) bek-

leszögezendő, hogy adatkezelő alatt olyan személyt értünk (legyen az akár költségvetési szerv, gazdasági társaság vagy épp magánszemély), aki vagy amely az adatkezelés céljait és eszközeit önállóan vagy másokkal együtt meghatározza, illetve az adatkezelésre vonatkozó döntéseket meghozza, míg adatfeldolgozó alatt olyan személyt, aki vagy amely az adatkezelő nevében, illetve megbízásából személyes adatokat kezel[84]. A gyakorlatban például az elkövetők azonosításához MI alapú szoftvert használó rendőrségi vagy nemzetbiztonsági szerv adatkezelőnek minősül, tekintettel arra, hogy az adatkezelés célját ezen szerv határozza meg, valamint hozza meg a kapcsolódó döntéseket (például: a rendszer alkalmazását, az érintettek azonosítását, velük szemben büntető eljárásjogi vagy nemzetbiztonsági tevékenységet érintő törvények szerinti intézkedések meghozatalát), míg a szerv által a szoftver technikai támogatása céljából igénybe vett informatikai cég vagy egyéb szakértői intézmény pusztán adatfeldolgozó lesz. Természetesen az adatkezelő és az adatfeldolgozó közötti szerződésnek tartalmaznia kell mindazon garanciákat, amelyek az adatkezelés biztonságát, valamint az érintettek jogait garantálják, ideértve például a felek közti együttműködést, titoktartást, érintetti kérelmek teljesítése során vagy adatvédelmi incidens esetén történő kapcsolattartást és feladatokat[85]. A szerződésben vagy annak mellékletében továbbá a feleknek részletesen javasolt rendelkezniük az adatfeldolgozótól elvárt szükséges adatbiztonsági intézkedésekről (például: megfelelő minőségű tűzfal és vírusírtó szoftverek garantálása, jelszómenedzsment stb.), ennek hiánya ugyanis az adatkezelő, valamint az érintettek tekintetében jelentős kockázattal járhat.

Természetesen előfordulhatnak olyan esetek is, ahol több adatkezelő határozza meg közösen az adatkezelés célját és eszközeit. Őket közös adatkezelőnek nevezzük, és esetükben elvárható, hogy a köztük lévő megállapodást írásba foglalják, valamint annak lényegét az érintettek számára is elérhetővé tegyék[86]. Tekintettel arra, hogy – az adatfeldolgozóval szemben – ezen felek mindegyike azonos vagy legalábbis jelentős súllyal rendelkezik az adatkezelés céljának, valamint a kapcsolódó döntések meghozatala tekintetében, így a

[84] GDPR 4. cikk 7-.8. pontok, Infotv. 3. § 9. és 18. pontjai

[85] Lásd: GDPR 28. cikk (3) bek.

[86] GDPR 26. cikk (1)-(2) bek.

felelősségük is egyetemleges az érintettel szemben, aki a közös adatkezelők bármelyikével szemben felléphet adatvédelmi jogainak esetleges megsértése esetén[87].

A fentieken túl, tekintettel arra, hogy az MI alapú adatkezelések az érintettek jogaira és szabadságaira nézve számos esetben magas kockázatokkal járnak, így esetükben az adatkezelő – figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljaira – köteles adatvédelmi hatásvizsgálatot végezni arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik [88]. A vizsgálatot a GDPR által előírt eseteken, így egyes személyes jellemzők módszeres és kiterjedt értékeléssel járó automatizált adatkezelésen, bűnügyi vagy különleges adatok nagy számban történő kezelésén, vagy nyilvános helyek nagymértékű, módszeres megfigyelésén[89] túl az adatkezelő bármely olyan esetben köteles elvégezni, ahol meglátásai szerint az adott adatkezelési művelet az érintettek jogaira vagy szabadságaira nézve magas kockázattal járhat (ideértve adott esetben például: okos eszközökkel kapcsolatos adatkezelés, bűnüldözési célból nagy számú személyes adat kezelése)[90]. Amennyiben pedig a hatásvizsgálat azt állapítja meg, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, úgy a személyes adatok kezelését megelőzően az adatkezelő köteles konzultálni a felügyeleti hatósággal[91].

4. A mesterséges intelligencia és az adatbiztonság

Napjainkban a személyes adatok informatikai környezetben történő tömeges kezelése során a hiányos adatbiztonsági intézkedések jelentik az egyik legnagyobb kockázati tényezőt az érintettek személyes adatainak védelme vonatkozásában. Mindez pedig különösen igaz az MI általi adatkezelésekre, tekintettel arra, hogy az MI alapú megoldások jellemzően automatizált módon működnek, így egy-egy adatbiztonsági probléma esetükben óriási kockázatokkal bírhat. Természetesen azonban az adatbiztonsági intézkedések alkalmazásának

[87] GDPR 26. cikk (3) bek.

[88] GDPR 35. cikk (1) bek.

[89] GDPR 35. cikk (3) bek.

[90] Ezen esetekre példaként szolgálnak a NAIH honlapján felsorolt esetek (lásd: https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) [2020.11.15.]

[91] Lásd: GDPR 36. cikk (1) bek.

követelménye nem csak informatikai elvárás, éppúgy részét képezi a papíralapú dokumentumok kezelésének ésszerű megszervezése, valamint a fizikai biztonság garantálása. Erre tekintettel az adatkezelőknek kiemelt figyelemmel kell lenniük az alábbiakra is:

- az MI alapú rendszereket kezelő, azokhoz hozzáférő munkavállalóik számára irányadó hozzáférési szabályzat megfogalmazása[92];
- az adatok és rendszerek fizikai tárolására szolgáló helyiségek védelmére;
- a rendszerekkel kapcsolatos hozzáférési jogok megfelelő szabályozása (például: jelszómenedzsment, admin-jogosultságok szűk körű kiosztása, titkosított kommunikáció)[93];
- az adatvédelmi incidensek kezelésével kapcsolatos szabályzat készítése, amely eligazítást nyújt arra az esetre is, hogy az egyes incidenseket mikor kell bejelenteni az adatvédelmi hatóságnak[94].

Mint az a fentiekből is látszik tehát, az MI alapú adatkezelések megszervezésének elengedhetetlen részét képezik az adatbiztonsági intézkedések és az azokkal kapcsolatos megfelelő részletességű belső szabályozás megléte.

5. A Belügyminisztérium, valamint az egyes alárendelt szervek MI alapú adatkezelésével kapcsolatos szempontok

Az MI alapú megoldások belügyi szervek általi alkalmazása mind az egyes szervek, mind a társadalom egésze számára számos előnnyel járhat (például: a döntések hatékony meghozatala, az ügyfelekkel történő kommunikáció támogatása, kibervédelmi megoldások). Ezek azonban nem érvényesülhetnek a személyes adatok, valamint a magánszféra védelmének rovására, így meg kell találni az egyensúlyt a fenti előnyök hatékony kihasználása és az érintettek jogainak és szabadságainak védelme között. Az alábbiakban hazai és nemzetközi példák alapján azt foglalom össze, hogyan is támogatható a belügyi

[92] A francia adatvédelmi hatóság adatbiztonsági intézkedésekkel kapcsolatos tájékoztató anyagja. Lásd: The CNIL's Guides – 2018 Edition, Security of personal data, 2018 („**CNIL Tájékoztató**"), 9. Elérhető:https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf [2020.11.15.]

[93] CNIL Tájékoztató 9-10., 12.

[94] NAIH/2020/1137. ügyszám alatt hozott határozata, 11.

szervek munkája MI alapú megoldásokkal, és ezen megoldások milyen adatvédelmi kihívásokkal járnak, azok hogyan is kezelhetők.

5.1. Rendészeti és nemzetbiztonsági szervek általi adatkezelések

A rendészeti, valamint nemzetbiztonsági szervek gyakorlatában az arcfelismerő rendszerek alkalmazása egyre fontosabb szempontot képez, az ilyen rendszerekkel ellátott térfigyelő kamerák pedig egyre kiterjedtebb mértékben vannak jelen a világ nagyvárosaiban. Ezen rendszerek alkalmazásánál különösen fontos szempontot képez:

- az adott rendszerekhez kapcsolódó algoritmusok „elfogultsági faktora", ehhez kapcsolódóan a rendszer által alapul vett személyes adatok köre, az értékelés, valamint a rendszer által végzett automatizált döntés meghozatalával kapcsolatos szempontok;
- a rendszer által meghozott döntések emberi felülvizsgálata;
- az érintettek joggyakorlási lehetőségei (ideértve akár a GDPR szerinti, akár a Infotv. szerinti érintetti jogok gyakorlását, amennyiben a rendszerrel történő adatkezelés bűnüldözési, nemzetbiztonsági célból történik);
- a rendszer „éles" alkalmazását megelőző tapasztalatok értékelése, az esetleges hiányosságok kiigazítása.

A fentiek kapcsán leszögezhető, hogy a rendszerek éles alkalmazás előtti tesztelése, valamint a folyamatos emberi felülvizsgálat garantálása kifejezetten erősítheti az arcfelismerő technológia pontosságát és hitelességét, míg ezek hiányossága komoly kockázatokhoz vezethet, és az ezen rendszerek mögötti társadalmi támogatottságot is meggyengítheti. A Big Brother Watch nevű brit, adatvédelmi jogok védelmével foglalkozó szervezet 2018-as tanulmánya szerint például a londoni Metropolitan Police Service nevű rendőrhatóság által alkalmazott automatizált arcfelismerési rendszerek – a rendőrhatóság által a szervezet megkeresésére az információszabadsággal kapcsolatos jogszabályi rendelkezések szerint szolgáltatott statisztikai kimutatások alapján – az elmúlt időszakban az esetek 98 százalékában tévesen azonosítottak keresett személyeket, ártatlan személyekre vonva a hatóság figyelmét (*Big Brother Watch 2018: 3, 25.*).

Mindennek kapcsán jól látható, hogy az arcfelismerő technológia alkalmazása esetén az eljáró hatóságoknak még a rendszer alkalmazása előtt fel kell mérnie a szóba jöhető

adatvédelmi és adatbiztonsági követelményeket, valamint azokat olyan módon kell kialakítania, hogy az a legkevesebb hibalehetőséggel dolgozva, és a lehető legkevesebb mértékben járjon káros behatással az érintettek magánéletére.

Hangsúlyozandó azonban, hogy a fentieken túl a különböző rendőrségi és nemzetbiztonsági szervek által alkalmazott rendszerek egyéb területeken is hatékonyan alkalmazhatók, ideértve például a bűnüldözési tevékenységet vagy akár mentési munkálatokat is. Ezek területén azonban az érintettek megfelelő előzetes tájékoztatása és az adatvédelem hatékony megszervezése éppúgy kulcsfontossággal bír, mint az arcfelismerő technológia fenti alkalmazásánál. Mindez pedig különösen igaz a különböző adatbázisokban vagy online felületeken lévő adatokból való profilok kialakítására, tekintettel arra, hogy az így létrehozott profilok a hatóságok által könnyen nyomon követhetők, és további elemzések céljából felhasználhatók (*Buzás 2018; 198*), amely az érintettek magánélethez fűződő jogára, valamint alapvető jogaira és szabadságaira különös sérelemmel járhat.

5.2. Önkormányzati és egyéb hatósági adatkezelések

Az MI alapú megoldások fenti rendészeti és nemzetbiztonsági célú alkalmazásán túl jelentős lehetőségek mutatkoznak a technológia önkormányzati és egyéb hatósági igazgatás területén való felhasználására. E körben kiemelhetők a különböző önkormányzati chatbot szolgáltatások, amelyek megkönnyítik az önkormányzati ügyintézést, megszüntetik a felesleges sorban állást, valamint drasztikusan csökkentik az ügyterhet. Erre jó példa az egyesült királyságbeli Newcastle városának önkormányzata, amely külön chatbot alkalmazásokkal rendelkezik például a hulladék-ügyintézés vagy a szociális ügyintézés területén[95]. Ennek kapcsán kiemelendő, hogy hasonló kezdeményezések Magyarországon is működnek[96], továbbá Magyarország Mesterséges Intelligencia Stratégiája célul tűzi ki az állami és önkormányzati igazgatásban való, technológiával kapcsolatos szabványosítás bevezetését 2025-ig[97].

Mindemellett az MI alapú technológiákat az önkormányzatok, valamint a különböző hatóságok a döntés-előkészítés és a vonatkozó adatgyűjtések területén is egyre gyakrabban

[95] Lásd: https://nccportal.newcastle.gov.uk/digital/user-story-1 [2020.11.15.]

[96] Magyarország MI Stratégiája, 7.

[97] Magyarország MI Stratégiája, 52.

használják, ideértve például a vízügyi igazgatás területét, ahol elsősorban a különböző vízügyi mérések elvégzéséhez jelenthet segítséget a mesterséges intelligencia (*Alanen 2019*).

6. Záró gondolatok

Mindent egybevetve megállapítható, hogy a mesterséges intelligencia az emberiség új korszakát hozta el, amely egyben az ember alkotóképességét is egy magasabb szintre emelte. Természetesen a mesterséges intelligenciának sohasem lehet feladata, hogy teljesen felváltsa az emberi munkát, azonban a technológia számos olyan feladat átvállalására képes, ahol adott esetben az emberi kreativitás korlátozott. Ilyennek minősülnek a nagyszámú adatok kezelésével, rendszerezésével járó feladatok, de egyre komolyabb szerep jut a mesterséges intelligenciának az ügyintézői feladatvégzés (például: chatbotok vagy digitális asszisztensek) vagy a biztonsági műveletek (például: arcfelismerés) területén is.

Tekintettel pedig a technológia adatközpontúságára, a mesterséges intelligencia kapcsán nem hangsúlyozható eléggé az érintetti jogokra és szabadságokra kellő figyelemmel lévő adatkezelési gyakorlat megszervezésének fontossága. Az adatkezelő ehhez fűződő kötelezettsége pedig nem tudható le önmagában az adatvédelmi tájékoztató tessék-lássék módon való elkészítésével, valamint az általa folytatott műveletek jogi értelemben vett „lepapírozásával". A megfelelő adatkezelői hozzáállás e tekintetben a technológia folyamatos figyelemmel kísérését, az esetleges hibák orvoslását és a jogszabályi és etikai követelményeknek való megfelelés nyomon követését jelenti, mindez pedig – az adatvédelmi hatósági gyakorlattal összhangban – különösen igaz a rendvédelmi és nemzetbiztonsági, valamint az egyéb belügyi szervekre, amelyek e körben példamutató magatartást kell, hogy tanúsítsanak[98], és a technológia megfelelő és hatékony alkalmazása mellett az adatvédelmi elvek érvényesítésével is élen kell járniuk.

[98] A NAIH/2019/2471/6 ügyszám alatt hozott határozata, 8. Ennek kapcsán a NAIH rendőrségi szerv tekintetében emelte ki, hogy az általa folytatott tevékenységre tekintettel elvárható az adatvédelmi tudatosság rendkívül magas szintje.

Irodalomjegyzék

ALANEN, P. (2019.02.14.) *How Artificial Intelligence Is Transforming The Water Sector: Case Ramboll*. SILO.AI. https://silo.ai/how-artificial-intelligence-is-transforming-the-water-sector-case-ramboll/ [Letöltve: 2020.11.15.].

ASIMOV, I. (1942) Runaround. *Astounding Science Fiction*, 03/1942.

Big Brother Watch: Face Off – The lawless growth of facial recognition in UK policing, May 2018, 3, 25. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf [Letöltve: 2020.11.15.]

BODA J. (2016) *„Szigorúan titkos!"? – Nemzetbiztonsági Almanach*. Budapest, Zrínyi Kiadó. pp. 126.

BŐGEL GY. (2017) Mi és a mesterséges intelligencia. *Valóság*, 60/11. pp. 2.

BUZÁS P. (2018) Az érintett jogai. In: Péterfalvi A. (ed.) *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer Hungary. pp. 198.

CAREY, S. (2018.03.16.) *How Sky is looking to recommend content according to your mood*. Computerworld. https://www.computerworld.com/article/3427637/how-sky-is-looking-to-recommend-content-according-to-your-mood.html [Letöltve: 2020.11.15.].

GASZT CS. (2019) A mesterséges intelligencia szabályozási kérdései, különös tekintettel a robotikára. *Infokommunikáció és jog*, 16/72. pp. 22.

KLEIN T. (2018) Robotok a beteggondozásban és a gyógyításban. In: Klein T. & Tóth A. (eds.) *Technológia jog – Robotjog – Cyberjog*. Budapest, Wolters Kluwer Hungary. pp. 211.

MISKOLCZI B., SZATHMÁRY Z. (2018) *Büntetőjogi kérdések az információk korában – mesterséges intelligencia, bigdata, profilozás*. Budapest, HVG-Orac Lap- és Könyvkiadó Kft. pp. 190-191.

NECZ D. (2018) A mesterséges intelligencia hatása a szerzői jogra. *Iparjogvédelmi és Szerzői Jogi Szemle*, 13/6. pp. 53.

Newcastle város egyes digitális szolgáltatásaival kapcsolatos tájékoztató oldala https://nccportal.newcastle.gov.uk/digital/user-story-1 [Letöltve: 2020.11.15.]

NICHOLS, G. (2016.02.11.) *Watch: In search of lost people, drones recognize and follow forest trails*. ZDNet. https://www.zdnet.com/article/watch-in-search-of-lost-people-drones-recognize-and-follow-forest-trails/ [Letöltve: 2020.11.15.].

PERECZ L. (2012) Internet, jog, információs társadalom. In: Pázmándi K. & Verebics J. (eds.) *E-jog*. Budapest, HVG-Orac Lap- és Könyvkiadó Kft. p. 22.

SZABÓ M. D., SZÉKELY I.– SIMON É. (2008) Az elektronikus személyazonosítás és ügyintézés adatvédelmi követelményei. In: Székely I. & Szabó M. D. (eds.) *Szabad adatok, védett adatok?* Budapest, Információs Társadalomért Alapítvány. pp. 154.

TURING, A. M. (1950) Computing Machinery and Intelligence. *Mind*, LIX/(1950)/236. pp. 433.

UDVARY S. (2018) Fémrabszolga vagy rivális életforma? A robotok jogi szabályozásának első lépései. *Gazdaság és jog*, 26/12. pp. 14.

ZŐDI ZS. (2018) A digitalizáció hatása a jogászi szakmára. *Gazdaság és Jog*, 26/12. pp. 8.