Kollár Gergő

A mesterséges intelligencia alkalmazásának adatvédelmi aggályai munkajogilag releváns helyzetekben*

ÖSSZEFOGLALÓ

Markáns és gyors fejlődést láthatunk a világban, ha algoritmizált megoldásokra gondolunk, s ezek a megoldások aktívan érintik a munka világát és a munkajog területét.[1] A Mesterséges Intelligencia (MI) – tágabban megfogalmazva az algoritmusvezérelt folyamatok – alkalmazási kérdéseinek alapvető aktualitását az információs technológia gyors fejlődése indukálja. Minden előnyével és hátrányával együtt ez kétségtelenül meghatározó tényező mind a köz-, mind a magánszféra szereplői számára. Ez teszi ugyanis lehetővé az olyan kiemelkedő teljesítmények mindennapos használatát, mint a cégalapításban közreműködő virtuális asszisztens (chatbot technológia, pl. UNA Litvániában[2]). Ekként válhatott a digitalizáció egyik központi célkitűzésévé az európai és hazai közigazgatásnak, gazdasági szereplőknél egyaránt.[3] Ennek a célkitűzésnek a COVID-19 járvány és az arra adott globális megoldási lehetőségek egyértelmű megerősítésül szolgáltak.[4]

A fejlődési cél szem előtt tartása mellett azonban nem szabad megfeledkezni a kockázatokról, amelyek különösen nagy hatást gyakorolhatnak például az emberi méltóságra és annak védelmére, a természetes személyek magánszférájába való aránytalan beavatkozás, valamint a személyes adataiknak nem megfelelő kezelése által. Jelen tanulmány célja a munkajogi környezetben használt MI rendszerek központi adatvédelmi aggályainak azonosítása. Ehhez a szükséges mértékben az ebben a környezetben alkalmazható algoritmusok jelenlegi és lehetséges felhasználási

* A tanulmány a 2020-1.1.2-PIACI-KFI-2021-00306 Okos Révkalauz HUB projekt keretében készült.

[1] A változás nem újkeletű, ld. Bankó Zoltán - Szőke Gergely László: *Issues of Digital Workplace: The Situation in Hungary.* Pécs, JURINFO, 2016. 31-38.o.

[2] *„UNA – the first virtual assistant of public administration in Latvia", Observatory of Public Sector Innovation (2018)* https://oecd-opsi.org/innovations/una-the-first-virtual-assistant-of-public-administration-in-latvia/ (2022.08.22.) illetve a chatbotok további használatáról: Hohmann Balázs: Chatbotok a kormányzati platformok szolgálatában: Alkalmazási követelmények és átláthatósági hatások. Belügyi Szemle, 71(4), 2023, 691-700. o.

[3] COM(2020) 65 final; COM(2020) 66 final

[4] Ennek hatásairól ld. pl. Hohmann Balázs: *The Impact of the Government's Restrictive Measures on the Transparency of the Administrative Proceeding in the Context of the COVID-19 Pandemic.* In: Hohmann Balázs - Shasivari, Jeton (szerk.): *Expanding Edges of Today's Administrative Law.* Bucharest, ADJURIS,2021. 154-160. o.

területeinek feltárására és az Általános Adatvédelmi Rendelet mesterséges intelligenciával kapcsolatos szabályozási megközelítésének vizsgálatára is sor kerül.

I. Bevezetés

A mesterséges intelligencia különös súlyát egyfelől a számítástechnika új lehetőségei és az egyre növekvő mennyiségű rendelkezésre álló adat adja, másfelől azonban meghatározó tényező a jelenségre adott döntéshozói reakció is. Európa feltett szándéka ugyanis, hogy „globális vezetővé váljon az adatgazdaság innovációja és alkalmazásai terén",[5] így az MI helyzetének rendezése nem pusztán innovatív természete miatt kiemelt jelentőségű, hanem a civil társadalmakban betöltendő szerepe miatt is. A digitális gazdaság megvalósítása a mai intenzíven változó világban egyébként is különös jelentőségre tett szert.

A munkajogi folyamatok működési mechanizmusai természetükből adódóan magas kockázatúnak tekinthetők, figyelembe véve az érintett munkavállalók magánéletébe erős behatást gyakorló és rendkívül változatos tevékenységi területeit, valamint az érintettek részvételi önkéntességének hiányát.[6] A kockázatok számbavételét követően is elmondható azonban, hogy a mukáltatóknak kulcsszerepet kell játszania az MI technológiák felvételében és biztonságos alkalmazásában. Az MI rendszerek által biztosított jobb elemzési képességek, folyamat-automatizációs lehetőségek, valamint a gyors és informatív visszacsatolások által várhatóan csökkenthetők az egyes szolgáltatások költségei, miközben színvonaluk és reagálási sebességük jelentősen növelhető.

II. Mesterséges intelligencia – alkalmazási lehetőségek és kockázatok

1. A mesterséges intelligencia és technológia háttere

A mesterséges intelligencia jelenségének lehatárolása, fogalmának megragadása még ma sem egyszerű feladat. Több irányból közelítve egymástól eltérő meghatározások születhetnek, anélkül, hogy egyik vagy másik objektíve „hibás" lenne. Egy számomra jól értelmezhető, egyszerű és kompakt megfogalmazás szerint a mesterséges intelligencia „olyan technológiák együttese, amelyek adatokat kombinálnak algoritmusokkal és számítási teljesítménnyel",[7] jellemzően folyamat-automatizációs célok elérése érdekében. Ebből egyértelműen kiolvasható a technológiai komplexitás és multidiszciplinaritás, valamint az adatalapúság és az algoritmus-vezérelt jelleg.

A fenti terminológia teljesebb körű pontosításához érdemes tisztázni, hogy az MI mely esetekben, milyen körülmények között és miért minősülhet aggályosnak. Másként megfogalmazva milyen jelek utalnak arra, hogy a kérdéses adatkezelési folyamat a kockázati skála egyik szélső értéke felé közelít. A jelek, amiket a magam részéről feltétlenül ide sorolnék azok az un. Big Data alapúság, illetve az adatosítás, a

[5] COM(2020) 65 final

[6] Agencia Española Protección Datos (AEPD): *Technologies and Data Protection in Public Administrations*. AEPD, Barcelona, 2020.

[7] COM(2020) 65 final

cloud computing és a Dolgok Internete jelenségek. Ezek mind egymással, mind az algoritmizált folyamatokkal nagy mértékben összefüggenek, de mint jelenségek önmagukban is kiterjedt vizsgálatra érdemesek, így e helyütt mindössze röviden, a téma szempontjából fontos aspektusaikra térek ki.

A Big Data, másnéven nagy adathalmazok, olyan hatalmas méretű adatkoncentrációk, valamint az azokon egyedülállóan komplex (skálázható) technológiai környezetben végzett számítástechnikai műveletek, amelyeket kiemelten a nagy adatmennyiség, az adatok változatossága, a feldolgozási sebesség és a változékonyság jellemez.[8] A mesterséges intelligencia ezen technológiai konstelláció eredményeként léphet át magasabb rendű, ám ezzel együtt kockázatosabb létszakaszába.

Alapvetően az input oldalt, tehát az adatgyűjtési lehetőségeket befolyásolja a Dolgok Internete (Internet of Things, IoT), amely az egymással IP[9] alapon kommunikáló és szenzorosan adatokat gyűjtő, valamint továbbító eszközöket jelenti.[10] Az adatosítás (datafikáció) egy olyan társadalmi szokás (trend), amely a mindennapi emberi magatartások digitális adattá történő átalakításának folyamatát jelenti.[11] Utóbbiak kifejezetten az új, korábban adatként nem létező adattípusok összegyűjtésével, illetve generálásával vesznek részt a folyamatban. Szintén megemlítendő az un. cloud computing,[12] ami a szükséges hardver erőforrás kiszervezését és azokhoz az interneten történő kapcsolódást jelenti.[13] Ez a gyakorlatban tipikusan külső tárhelyszolgáltatások formájában valósul meg és a magas adatkoncentrációból eredő adatvédelmi és adatbiztonsági kockázatokon túl igényérvényesítési akadályokat is előidézhet a jellemzően országhatárokon átnyúló adatmegosztási szisztéma miatt.[14]

2. Az adatvédelmi jog előírásai a mesterséges intelligencia technológia alkalmazásával összefüggésben

2.1. Az adatvédelem és az algoritmizált folyamatok kapcsolata

Az adatvédelmi jog – vagyis a személyes adatok védelméhez fűződő alapvető emberi jog felett őrködő szabályok összessége[15] – több ponton gyakorol hatást az eddigiekben taglalt technológiai és társadalmi folyamatok alakulására. Mielőtt a hatályos joganyag vizsgálatára rátérnénk érdemes néhány korszaktól és szabályozási rezsimtől független megállapítást tennünk a tisztánlátás érdekében. Látni kell ugyanis, hogy az

[8] „ISO/IEC 20546:2019" Information Technology – Big Data – Overview and vocabulary, 3.1.2. pont
[9] Az internetprotokoll, az interneten keresztüli kommunikáció egyik alapvető szabványa
[10] Techopedia: What Does internet of Thnigs (IoT) Mean? https://www.techopedia.com/definition/28247/internet-of-things-iot (2022.08.22.)
[11] Southerton, Clare: Datafication. Schintler, Laurie – McNeely, Connie (Szerk.): *Encyclopedia of Big Data*. Springer, Cham, 2020. 1-4 o. https://doi.org/10.1007/978-3-319-32001-4_332-1
[12] Magyarul használatosak a „számítási felhő" és a „felhőtechnológia" kifejezések
[13] Techopedia: Cloud Computing, https://www.techopedia.com/definition/2/cloud-computing (2022.08.22.)
[14] Bankó Zoltán – Szőke Gergely László: Az információtechnológia hatása a munkavégzésre. Utilitates., Pécs, 2015. 22. o.
[15] Jóri András: Adatvédelmi Kézikönyv, Elmélet, Történet, Kommentár. Osiris Kiadó, Budapest, 2005. 17 o.

adatvédelmi jog szabályozási spektruma sokkalta szélesebb az algoritmizált folyamatok területénél, így a hatásgyakorlás is viszonylag közvetett módon valósul meg.

Az MI rendszerek alkalmazásával kapcsolatban – adatvédelmi szempontból – két fontos szakaszt szükséges elkülönítenünk egymástól,[16] annak érdekében, hogy az aggályok értelmezhetőek legyenek. Az első szakasz a fejlesztés időszaka, ez a rendszer felépítésének folyamata, vagyis egy olyan tevékenység, aminek eredményeként működő MI rendszer jön létre. Jelen esetben a kapcsolódási pont az adatvédelem és az MI között a fejlesztéshez használt adathalmaz (training data) forrása és jogi megítélése lesz.[17] Ez az adathalmaz a gépi tanulás minden formájához (felügyelt, felügyelet nélküli, megerősített, mély tanulás) szükséges, mivel a mesterséges neurális háló kialakulásához szükséges input adatokat szolgáltatja.[18] A konkrét kapcsolat az adatvédelemmel akkor jön létre, amikor ez az adathalmaz személyes adatokat[19] is tartalmaz, hiszen a GDPR 2. cikk szerinti tárgyi hatály meghatározása szerint a rendelet alkalmazandó minden „személyes adat részben vagy egészben automatizált módon történő kezelésére". Ez természetesen önmagában nem aggályos, a nehézséget kevésbé a training data jogi megítélése okozza (bár kétségtelenül az ilyen helyzetek kialakulásának előfeltétele, hiszen személyes adat hiányában semmilyen adatvédelmi aggály nem merülhet fel), sokkal inkább annak forrása, illetve pontos ismerete. A tendencia jelenleg ugyanis azt mutatja, hogy az ilyen „feltanításhoz" használt adathalmazok forrása nagyarányban az un. Big Data, vagyis a korábban már bemutatott nagy adathalmazok.[20] Ennek a következtében pedig a fejlesztési szakasz input adatai többnyire átláthatatlanok még a fejlesztők számára is, a kezelésük pedig ennek megfelelően rendkívül nehézkes, hiszen ebben az esetben az adatokról még az sem állapítható meg egyértelműen, hogy személyes adatnak minősülnek-e.[21]

A második szakasz a fejlesztés végeztével az alkalmazás (deployment) időszaka, vagyis az MI rendszer valós környezetben történő használata. Az input adatok nagyban eltérnek az egyes MI rendszerek típusától függően, így a kategória alkotás valamivel általánosabb módon történhet csak meg. Annyi bizonyosan elmondható, hogy az adatok forrása nem feltétlenül Big Data (csak akkor, ha az MI feladata nagy adathalmazok elemzése). Továbbá jó eséllyel az adatok jogi megítélése és forrása az elvégzendő feladattal állnak összefüggésben, így például az önvezető hókotró a környezetének vizuális input adatait fogja felhasználni a tájékozódáshoz, a nyelvhelyességet ellenőrző szoftver a bevitt írott szöveget vizsgálja, míg egy robotbíró az előtte lévő ügy iratait elemzi következtetések levonásához és a döntések meghozatalához. Ezek az adatok láthatóan nagy eltérést mutathatnak egymáshoz képest, illetve eshetőlegesen

---

[16] UNESCO: First draft of the recommendation on the ethics of artificial intelligence, shs/bio/aheg-ai/2020/4 rev.2 (2020) 4. o.

[17] European Parliamentary Research Service, Scientific Foresight Unit (STOA): The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (PE 641.530 – June 2020) 15. o.

[18] Fejes Erzsébet – Futó Iván: i.m. 30-32. o.

[19] Közvetlen vagy közvetett módon azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.

[20] Siapka, Anastasia: The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI. Panteion Társadalom- és Államtudományi Egyetem (2018) 19-22. o. https://doi.org/10.2139/ssrn.3408773

[21] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 15- 30. o.

tartalmaznak személyes adatokat a feladattól függően. Közös bennük azonban (a fejlesztési szakasztól eltérően) a nagyobb fokú átláthatóság. A működő MI ugyanis a feladat elvégzéséhez szolgáltatott input adatokon fog „dolgozni", így azoknak a jogi megítélése feltárható (a hókotró nem feltétlenül kezel személyes adatot, míg a robotbíró jellemzően igen), a forrásuk pedig a működéssel érintett terület (a hókotró esetén a repülőgép kifutópályája, a robotbíró esetén a jogi eljárás). Ezzel összefüggésben egészen más aggályok merülnek fel az alkalmazási szakaszban, mint a fejlesztési szakaszban, azonban összességében elmondható, hogy mindkét esetben az adatvédelmi szabályok alkalmazása nincs kizárva, így az előírások minden esetben figyelembe veendők.[22]

2.2. A vonatkozó adatvédelmi előírások

Az adatvédelmi jog 1970-es években kezdődő kialakulásától kezdve mind a mai napig a technológia fejlődésére adott jogalkotói válasz egyik megvalósulása, így a különböző időszakok eltérően, de legalábbis eltérő súllyal határozták meg a jogpolitikai célokat.[23] Azonban minden szabályozási generáción átívelő motívum az információs egyensúlytalanság („információs túlhatalom") kialakulásának korlátozása, illetve hátrányos következményeinek mérséklése.[24] Az idők folyamán az információs hatalom birtokosának személye együtt változott az adatvédelem szabályozási eszközeivel. Ez a hatalom kezdetekben az államoknál volt, majd fokozatosan beléptek a magánvállalatok is, így a legkorábbi tisztán átláthatóságot és garanciális szabályokat megállapító rendelkezéseket egyre nagyobb mértékben bővítették az adatalany oldalán megjelenő jogokkal. Ezek a jogok az életviszonyok egyre bonyolultabbá válásával formálódtak mind komplexebbé, így lehetséges, hogy az idő előrehaladtával egyre több jogalappal (ami egy speciális jogi felhatalmazás az adatok kezelésére,[25] tehát az adatkezelés megkezdésének egyik előfeltétele[26]) és az érintetti jogok egyre szélesebb skálájával szembesülünk.

Az Általános Adatvédelmi Rendelet[27] 2018 óta alkotja az európai adatvédelmi jog gerincét. Jogforrási formájából következtethetünk a jogalkotói hozzáállás fordulatára, tekintve, hogy korábban a területet egy irányelv[28] szabályozta, jelenleg pedig egy közvetlenül hatályos, közvetlenül alkalmazandó uniós rendelet (bár számos az

---

[22] Uo. 15-30. o.

[23] Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése. Infokommunikáció és jog 2013/3, 107-111. o.

[24] Szabó Máté Dániel: Az információs hatalom alkotmányos korlátai. Miskolci Egyetem, Miskolc, 2012. 11-29. o.

[25] Péterfalvi Attila – Révész Balázs – Buzás Péter (Szerk.): *Magyarázat a GDPR-ról*. Wolters Kluwer, Budapest, 2018. 111 o.

[26] Az Európai Unió Alapjogi Ügynöksége és az Európa Tanács: *Európai adatvédelmi jogi kézikönyv*. Az Európai Unió kiadóhivatala, Luxembourg, 2019. 158 o.

[27] Az Európai Parlament és a Tanács (EU) 2016/679 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 szóló rendelete

[28] Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló irányelve (adatvédelmi irányelv)

irányelvből átvett megoldást alkalmaz továbbra is[29]). Ebből fakadóan az uniós jog és jogalkalmazás egységesebb, mivel kevesebb mozgástér maradt a tagállami jog divergenciájára. A Rendelet és az azt helyenként kiegészítő, pontosító tagállami jog[30] számtalan alkalmazandó rendelkezést tartalmaz, azonban ezek egyike sem expressis verbis előírás az MI rendszerekre.[31] A legszorosabb kapcsolat a GDPR profilalkotás[32] és automatizált döntéshozatal[33] fogalmaival áll fenn, továbbá a Rendelet alapelvei,[34] a jogalapok[35] és az érintetti jogok,[36] szintén különös figyelmet érdemelnek. Kiemelendő még a beépített és alapértelmezett adatvédelem elvének megfelelő követelményrendszer,[37] illetve a közérdekű archiválás, tudományos és történelmi kutatás, valamint statisztikai célok, mint az adatkezelés különös esetei.[38] Az aggályokkal kapcsolatban a releváns rendelkezések vizsgálatára alább kerül sor, itt csak a profilalkotást és az automatizált döntéshozatalt tekintem át, különös relevanciája miatt.

A profilalkotás a GDPR szerint személyes adatok automatizált kezelésének bármely formája lehet, amely során az adatokat egy természetes személy jellemzőinek értékelésére, mozgásához kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.[39] Másként megfogalmazva a profilalkotás adatok közötti összefüggések azonosítása és konkrét csoportokra vagy személyekre történő értelmezése, olyan kategóriák létrehozása érdekében, amelyek azonos tulajdonságokkal rendelkeznek.[40] Az automatizált döntés ehhez képest egyszerűbben megragadható, mindössze egy kizárólag automatizált adatkezelésen alapuló döntést jelent.[41] Utóbbival a 22. cikk kapcsán részletesen foglalkozok, előbbiről viszont néhány általános megállapítást teszek. A GDPR leginkább korlátokat állít fel a profilalkotással kapcsolatban, ezt egyfelől az érintetti jogokon (tájékoztatás, tiltakozás), másfelől az alapelveken (adattakarékosság) keresztül teszi, fontos leszögezni azonban, hogy a profilalkotás egyáltalán nem minősül tiltott tevékenységnek a GDPR szabályozási rendszerében, hiszen bármilyen jogalapon végezhető, amennyiben az adatkezelés egyéb feltételei fennállnak.[42] A korlátozás mögötti jogpolitikai cél a profilokban rejlő veszélyek enyhítését célozza, mivel bizonyos helyzetekben megfoszthatja önmeghatározási képességétől az egyént, továbbá a Big Data alapú rendszerek megjelenésével gyakorlatilag végtelen számú adat alapján képesek

[29] Kis Kelemen Bence – Hohmann Balázs: A Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra. *Infokommunikációs jog*, 2016/2., 64-66. o.
[30] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info.tv.)
[31] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 35. o.
[32] GDPR 4. cikk 4. pont
[33] GDPR 22. cikk
[34] GDPR 5. cikk
[35] GDPR 6. cikk
[36] GDPR 12-22. cikkei
[37] GDPR 25. cikk
[38] GDPR 89. cikk
[39] GDPR (71) preambulumbekezdése és 4. cikk 4. pontja
[40] Pataki Gábor – Szőke Gergely László: *Az online személyiségprofilok jelentősége*. In: Polyák Gábor (Szerk.): *Algoritmusok, keresők, közösségi oldalak és a jog – a forgalomirányító szolgáltatások szabályozása*. HVG-ORAC, Budapest, 2020. 75. o.
[41] GDPR 22. cikk (1) bekezdés
[42] Jóri András: *A GDPR magyarázata*. HVG-ORAC, Budapest, 2018.

kialakítani egyre bonyolultabb profilokat. Az ilyen profilok létezése pedig visszaélésre alkalmas helyzetbe hozhatja az ismeretanyagát birtokló személyeket, ezzel súlyosan veszélyeztetve az érintett magánéletének különböző aspektusait.[43]

3. Adatvédelmi aggályok az MI rendszerekkel kapcsolatban

3.1. Az aggályokról általában

Az adatvédelmi jog alapvető célkitűzései és az MI rendszerek által támogatott – különösen a Big Data alapú – adatfeldolgozási mechanizmusok tagadhatatlanul kollíziós pályán mozognak egymás viszonylatában.[44] Ezek a rendszerek mindenkori működési elvük szerint a lehető legnagyobb adathalmazhoz történő hozzáférést igénylik, ennek megfelelően az adatok gyűjtésekor sem szívesen vannak tekintettel az olyan korlátozásokra, mint a célhoz kötöttség, adattakarékosság vagy korlátozott tárolhatóság.[45] Ez abból az egyszerű törvényszerűségből ered, hogy az adatgyűjtés pillanatában nem szükséges (és nem is lehetséges) teljes körűen tisztában lenni a lehetséges felhasználási / hasznosulási lehetőségekkel, ugyanis ezeket az MI rendszer maga fogja kimunkálni ismeretlen összefüggések megtalálásával és új következtetések levonásával. Tehát az első és legfontosabb adatvédelmi aggály a jogpolitikai célok és a technológia működési elvének összeütközéséből ered. Ez önmagában nem jelenti, hogy a GDPR végérvényesen inkompatibilis lenne a Big Data alapú MI rendszerekkel, azonban az összeütközés feloldása komolyabb, esetről estre történő átgondolást igényel.[46]

Az előbbihez hasonló generálisan jelenlévő aggály a legtöbb fejlett MI rendszer immanens részét képező, un. fekete doboz (black box) jelenségből ered. A jelenség lényege, hogy az algoritmus működése során az input oldal és az output oldal közötti követhető kapcsolat megszűnik a külső szemlélő számára. Vagyis ezekben az esetekben tisztázott a bemeneti és kimeneti oldal adattartalma (az, hogy milyen adatok alapján, milyen eredmény jött létre), de a kettő közötti ok-okozati összefüggés (miért ez az eredmény jött létre a megadott adatok alapján) nem, vagy csak nagyon nehezen ismerhető meg.[47] Ez adatvédelmi szempontból alapelvi szinten okoz problémákat az átláthatóság hiánya miatt, de az érintetti jogok tiszteletben tartása és jogérvényesítés elősegítése is komoly akadályokba ütközhet. Az adatvédelmi megfontolások mellett egyéb alapvető emberi jogok (emberi méltóság, egyenlő bánásmód) is veszélyeztettek lehetnek, továbbá ágazati és eljárási szabályok is sérülhetnek.[48]

A harmadik olyan aggály, ami a teljes szisztémát áthatja az un. „algorithmic bias", amit magyarul algoritmizált elfogultságként fordíthatunk. Ebben az esetben

---

[43] Ződi Zsolt: Platformok, robotok és a jog. Gondolat Kiadó, Budapest, 2018. 86. o.
[44] Cohen, Julie E.: What privacy is for. *Harvard Law Review* 2013/126. 12-14. o.
[45] Mayer-Schönberger, Viktor – Cukier, Kennethe: *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston, Houghton Mifflin Harcourt, 2013. 26. o.
[46] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 44-45. o.
[47] Agencia Española Protección Datos (AEPD): i.m.
[48] Mohay Ágoston: *A mesterséges intelligencia szabályozási perspektívái az Európai Unióban*. In: Kis Kelemen Bence – Mohay Ágoston (Szerk.): *A technológiai fejlődés jogi kihívásai: Kézikönyv a jogalkotás és jogalkalmazás számára.* Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021. 72. o.

szoftverhiba vagy a fejlesztéskor használt training data torzítása / torzulása vezet az MI rendszer diszkriminatív működéséhez. Ez jóhiszeműséget feltételezve természetesen nem szándékolt hatás a fejlesztők részéről, hiszen könnyen elképzelhető (főleg történelmi adatbázisok esetén[49]), hogy egy olyan régóta meglévő, de ez idáig azonosítatlan megkülönböztető gyakorlat az ok, amit az algoritmus mindössze felerősített.[50] Adatvédelmi szempontból (az egyéb alapjogsérelem mellett) súlyos következményekkel járhat az ilyen diszfunkcionális működés – függetlenül az októl és a szándéktól – hiszen egy hátrányosan megkülönböztető módon működő algoritmus alapján meghozott döntés óhatatlanul jogellenes adatkezelést fog megvalósítani.[51]

3.2. Az MI és a GDPR alapelvei

A GDPR alapelvi rendszere igyekszik útmutatással szolgálni az értelmezési nehézségek elhárítására és a joghézagok feltöltésére, e tekintetben álláspontom rendkívül szerint jól látja el feladatát. Meggyőződésem, hogy az adatvédelmi jog valós elvárásainak megértéséhez az alapelvek megértésén keresztül vezet az út, így az aggályok részletes vizsgálatát is ezen ponton érdemes elkezdeni.

3.2.1. Jogszerűség, tisztességes eljárás és átláthatóság elve

Általában, és így az MI rendszerek esetén is, a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.[52] Az alapelv szerint az adatkezelés csak abban az esetben tekinthető jogszerűnek, ha az általánosságban is megvalósul,[53] így nemcsak az adatvédelmi tárgyú jogszabályoknak, hanem bármely egyéb személyes adatokat érintő normának is megfelel, így messzemenően tekintettel kell lenni az ágazati és eljárási rendelkezésekre, amelyek személyes adatokat érintenek. Jogszerűség egyik kiemelt előfeltétele az érvényes adatkezelési jogalap megléte,[54] amelyekről részletes vizsgálat a 4.3. pontban található. Az eljárás igazán abban az esetben tekinthető tisztességesnek, amennyiben az az érintetti jogokat magába foglalja és az érintettek jogérvényesítését aktívan (kérések és panaszok kezelése) és passzívan (előzetes tájékoztatás) is elősegíti, így látható, hogy szoros kapcsolatban áll az átláthatóság követelményével, amely alatt mindenekelőtt az érintettek számára egyértelműen meghatározható adatkezelési folyamatok kialakítása és az arról való tájékoztatás (ami tömör, könnyen hozzáférhető és könnyen érthető,

[49] Edwards, Lilian: Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions?. *IEEE Security & Privacy 16*(3), 2018, 46-48 o. https://doi.org/10.1109/MSP.2018.2701152
[50] Chander, Anupam: The Racist Algorithm?. *Michigan Law review, 115*(6), 2017. 1028-1030 o.
[51] BBC News: *Artificial intelligence: Algorithms face scrutiny over potential bias (2019).* https://www.bbc.com/news/technology-47638916
[52] GDPR 5. cikk (1) bekezdés a) pont
[53] Révész Balázs: Péterfalvi Attila – Révész Balázs – Buzás Péter (Szerk.): i.m. 95-96. o.
[54] Péterfalvi Attila – Révész Balázs – Buzás Péter (Szerk.): i.m. 95. o.

valamint világos és közérthető nyelven megfogalmazott[55]) értendő. Ezek a rendelkezések erőteljes átláthatóságot erősítő jelleggel rendelkeznek.[56]

A tisztességgel kapcsolatban MI rendszerek esetén fontos megkülönböztetnünk az információs tisztességességet és a szubsztantív (lényegi) tisztességességet.[57] Előbbi követelménye, a téves, hiányos, félrevezető tájékoztatás hiánya, vagyis az a kívánatos állapot, amikor az érintett minden szükséges információval rendelkezik az adatkezelést illetően.[58] Ezzel kapcsolatban rögtön egy sokat emlegetett aggály merül fel, ami szerint nincs arra garancia, hogy az érintett a kapott információt értelmezni is tudja. Ez főként ezen a területen lehet igaz, hiszen egy MI rendszer belső működése laikusok számára – nem meglepő módon – nehezen átlátható.[59] Utóbbi, vagyis a szubsztantív tisztességesség lényegét tekintve az eredmény tisztességességét várja el, vagyis az elfogultság és a diszkrimináció hiányát.[60] A GDPR (71) preambulumbekezdése a tisztességességet, mint adatkezelői kötelezettséget megalapítja, azonban előfordulhatnak olyan helyzetek, amelyekben akár a fekete doboz jelenségből, akár más okból kifolyólag a tisztességtelen adatkezelés ebbéli jellege rejtve marad még az adatkezelő elől is, így a jogellenes helyzet hosszú időn keresztül megoldatlan maradhat.

3.2.2. Célhoz kötöttség elve

Személyes adatokat csak meghatározott, egyértelmű és jogszerű célból lehet kezelni, továbbá az adatokat az eredeti céllal össze nem egyeztethető módon tilos kezelni.[61] Ez az alapelv a munkajogi viszonyokban is kifejezett érvényesülést kíván. Az alapelv megköveteli, hogy személyes adatokat csak az előre meghatározott cél megvalósulásához szükséges mértékben és ideig kezeljék. A probléma egyértelműen megmutatkozik adatok – nagy adathalmazokra jellemző – készletező típusú gyűjtésekor,[62] illetve ismeretlen eredetű adatok újra-feldolgozásakor, vagyis akkor, amikor nem vagyunk tisztában az eredeti adatkezelési céllal. Ide kapcsolódó fontos kivételszabályt alkot a Rendelet, amikor az 5. cikk (1) bekezdés b) pont második fordulatával összeegyeztethetőségi vélelmet állít fel. E szerint összeegyeztethető az eredeti céllal a 89. cikk (1) bekezdés szerinti közérdekű archiválás céljából, tudományos

---

55 GDPR (58) preambulumbekezdése

56 Megjegyezve azt, hogy az átláthatóság adatvédelmi területen alapelvi jelentőséggel is felmerül, de közjogi viszonyokban, hatósági eljárásban (akár munkajogi, akár adatvédelmi hatósági eljárásról legyen szó, ennél differenciált értelmezése szükséges, ld:
Hohmann Balázs: *The interpretation of transparency from the legal point of view*. In: Haffner, Tamás (Szerk.) IV. *Fiatalok EUrópában Konferencia -Tanulmánykötet*. Pécs, Sopianae Kulturális Egyesület, 2018. 155-163. o., illetve Hohmann Balázs: *Az átláthatóság értelmezése és követelményrendszere a közigazgatási hatósági eljárások tükrében*. Pécs, Novissima Kiadó, 2022. 76-85. o.

57 European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 44. o.

58 GDPR (60) preambulumbekezdése

59 Wachter, Sandra - Mittelstadt, Brent – Russel, Chris,: Counterfactual explanations without opening the black box: automated decisions and the GDPR. *Harvard Journal of Law & Technology Volume 31*(2), 2018. 842-843. o. https://doi.org/10.2139/ssrn.3063289

60 GDPR (71) preambulumbekezdés

61 GDPR 5. cikk (1) bekezdés b) pont

62 Siapka, Anastasia: i.m.47-48. o.

és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés. A kivételszabály alkalmazhatóságágának megítélése alapvetően nehéz ismeretlen eredetű adatok esetén, de még az eredeti cél ismeretében is különös vizsgálatnak kell alávetni a kompatibilitásukat. A 29. cikk szerinti munkacsoport állásfoglalása szerint átgondolandó a két cél közötti távolság, az új cél és az érintett várakozása közti viszony, az adat természete és annak az érintett érdekeire gyakorolt hatása, valamint a tisztességes adatkezelés elérése érdekébe az adatkezelő által alkalmazott védelmi intézkedések jellege.[63] Az aggályokkal kapcsolatban külön is kiemelendő, hogy a fejlesztési szakasz training adatállományba rendezetlen körülmények között bekerülő személyes adatok további felhasználása egyes személyekre és/vagy csoportokra vonatkoztatva hátrányos következményekkel járhat, amennyiben (bármely okból) téves következtetésekre döntés is alapul.

3.2.3. Adattakarékosság elve

Az adatkezelésnek mindig a korábban meghatározott céloknak megfelelőnek és relevánsnak kell lennie, továbbá szükséges mértékre kell korlátozódnia.[64] Az alapelvnek megfelelően kerülni kell a felesleges, értelmezhetetlen vagy előre meg nem határozott, jövőbeni célhoz kapcsolódó adatok kezelését. Kétségtelen feszültség látható az adattakarékosság és a Big Data alapú MI rendszerek között, ahogy azt fentebb már kifejtettem. A megoldást megfelelő jogértelmezéssel több-kevesebb sikerrel oldja meg a gyakorlat, mivel az adattakarékosság elve nem explicit számtani előírás, hanem jogelvként érvényesül minden adatkezelési folyamatban. Így a megfelelőség, relevancia és szükséges mérték fogalmait a várható előnyökkel és kockázatokkal arányos módon lehet értelmezni, ezzel egy lazább és könnyebben betartható követelménynek kell mindössze megfelelni. Ezen értelmezés szerint mindaddig bővíthető az adatkör ameddig az olyan mértékben járul hozzá a cél eléréséhez, amely előnyben részesítendő az új adatok bekerülésével létrejövő kockázatokhoz képest.[65]

3.2.4. Pontosság elve

Az elv szerint az adatokat a kezelésük során pontos és naprakész állapotban kell tartani és minden szükséges intézkedést meg kell tenni annak érdekében, hogy a pontatlan adatok törlésre vagy helyesbítésre kerüljenek.[66] A kockázatok e tekintetben kevésbé elvontak, jól érzékelhető, hogy pontatlan adatokkal semmilyen cél nem érhető

[63] Article 29 Data Protection Working Party: *Opinion 03/2013 on purpose limitation (WP203)*. 20-37. o.
[64] GDPR 5. cikk (1) bekezdés c) pont
[65] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 47-48. o.
[66] GDPR 5. cikk (1) bekezdés d) pont

el. Míg a fejlesztési szakaszban hibás logikai kapcsolatok kialakulásához, az alkalmazáskor helytelen következtetésekhez és téves döntésekhez vezethet.

3.2.5. Korlátozott tárolhatóság elve

A személyes adatok tárolása csak a cél megvalósításához szükséges ideig megengedett.[67] Az alapelvnek megfelelően az adatok kezelésének időben mindig meghatározottnak kell lennie, illetve semmilyen személyes adat sem kezelhető előre meghatározott időkorlát nélkül. A feszültség szintén érzékelhető az MI rendszerek készletező jellegű „jó lesz még valamire" szemlélete és az adatvédelmi jog elvárásai között. Különösen aggályosak azok a fejlesztési szakaszban lévő esetek, amikor az eredeti adat eredete és így a bekerülés ideje, valamint az előirányzott törlési ideje is ismeretlen.

3.3. Az MI és az adatkezelési jogalapok

Az adatkezelési jogalapok az adatkezelési folyamatokban megkülönböztetett szerepet töltenek be, ezt hathatósan tükrözi a GDPR 6. cikkének címe – ahol a jogalapok rögzítésre kerültek – ami az adatkezelés jogszerűsége. Ahogy arra már utaltam, a jogalap egy speciális jog általi felhatalmazás személyes adatok kezelésére, ezért minden esetben, minden adatkezelési folyamatnak rendelkeznie kell egy (pontosan egy) jogalappal.[68]

3.3.1. Az adatkezelés az érintett hozzájárulásán alapul

Az érintetti hozzájárulás hosszú múltra visszatekintő jogalap, a klasszikus értelemben vett információs önrendelkezés alapkövének tekinthető. Ennek megfelelően az érintett erős jogosítványokkal rendelkezik (hozzájárulás visszavonása, törléshez való jog), valamint számos garanciális szabály őrködik a hozzájárulás önrendelkezést biztosító jellege felett (önkéntesség, meghatározottság, kifejezett és félreérthetetlen jelleg[69]). A hozzájárulás bekérésének lehetséges esetei gyakorlatilag végtelenek, azonban a valódi és jogszerű hozzájárulás minden feltételének megfelelő nyilatkozatok, különösen a munkajogviszony alá-fölé rendeltségére tekintettel – véleményem szerint – ritkák, így bár ez a jogalap rendkívül sűrűn használt, számos jogi buktatóval kell számolnia az adatkezelőnek. Az MI rendszerek esetén sincs ez másként. Pozitívum, hogy a jogalap alkalmazható a fejlesztési és alkalmazási fázisban is, azonban mindkét esetben körültekintően kell eljárni. Elképzelhető, hogy az újra-hasznosított adatbázisok esetén az eredeti adatkezeléshez bekért hozzájárulás széles körű volt (un. broad consent), így bele tartozhat az ott megadott adatok új, de az érintett érdekeit nem sértő célokra történő felhasználása (itt is kérdéses az érintett képessége – még a szükséges tájékoztatás birtokában is – a lehetséges következmények értelmezésére, így okkal éri

[67] GDPR 5. cikk (1) bekezdés e) pont
[68] Péterfalvi Attila, Révész Balázs, Buzás Péter (Szerk.): i.m. 111 o.
[69] GDPR 7. cikk

egyre több kritika un. „notice and consent" eljárást[70]). Valamivel biztosabb alapokon nyugszik az adatkezelés az alkalmazási szakaszban, ha az adatkezelő a folyamat megkezdése előtt megfelelő hozzájárulással indítja az adatgyűjtést. Mindkét esetben komoly kihívás minden elvárásnak megfelelő hozzájárulást produkálni, utóbbival kapcsolatban könnyebbség, hogy nem kell egy másik adatkezelő eljárásának jogszerűségére hagyatkozni. A jogalappal kapcsolatban szintén érdemes figyelembe venni a hozzájárulás visszavonásának és az adatok törlésének lehetőségét, amit az érintett bármikor kérhet. Bármelyik jog gyakorlása okozhatja a folyamat-automatizáció megszakadását, szélsőséges esetben pedig a modell használhatatlanná válását.

3.3.2. Az adatkezelés szerződés teljesítéséhez szükséges

A „valamihez szükséges" típusú jogalapok közül az első mikor az adatokat szerződés teljesítése (vagy előkészítése) érdekében kezeljük. A jogalap esetén buktató lehet a szükségesség, mivel csak akkor alkalmazható, ha az adatkezelés a vállalt kötelezettség teljesítéséhez (szorosan) kapcsolódik. Szintén akadály lehet, hogy az érintett csak szerződő fél lehet, amennyiben nem minősül annak, a jogalap nem alkalmazható.[71] Fejlesztési szakaszban érezhetően nehezebb elképzelni, hogy az előbbi két feltétel fennálljon, azonban az MI rendszer alkalmazásakor már lehetséges magát az algoritmust a szerződéses rendelkezések részévé tenni.

3.3.3. Az adatkezelés jogi kötelezettség teljesítéséhez szükséges

Ezzel a jogalappal kapcsolatban rövidebb okfejtés is elégséges. Kijelenthető, hogy amennyiben kellőképpen pontosan került meghatározásra a jogszabályi kötelezettség,[72] az adatkezelő nem mérlegelhet, azt végre kell hajtania.

3.3.4. Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges

Ennek a jogalapnak az alkalmazhatósága általában limitált és ez igaz az MI rendszerekkel kapcsolatban is. Célja az élet, a testi épség és az egészség védelme érdekében szükséges adatkezelések lehetővé tétele, ezt azonban nagyon szűken

[70] Solove, Daniel J.: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, 2013/126. 1880-1882. o.
[71] Jóri András: i.m.
[72] Vagyis az Info.tv. 5. § (3) bekezdés előírásainak megfelel

értelmezi a gyakorlat. A „veszélynek" valódinak és közelinek kell lennie, veszélyeztetettség általános elhárítására kevésbé alkalmazható.[73]

3.3.5. Az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges

Ezt a jogalapot a jogi kötelezettséghez hasonlóan szintén valamilyen tagállami vagy uniós jognak kell meghatároznia, bár az előírásnak nem kell explicitnek lennie, elég, ha adatok kezelését teszi szükségessé. Fontos még, hogy szükségesnek kell lennie a feladat ellátásához vagy a jogosítvány gyakorlásához, valamint a feladat ellátás által kitűzött cél elérésével arányban kell állnia.[74] A jogszerűség eléréséhez természetesen a szükségességet és arányosságot részletesen vizsgálni kell (ami nem egyszerű feladat), valamint az adatkezelést jognak kell meghatároznia (ami nem feltétlenül létezik), de úgy gondolom még így is a legjobban alkalmazható az MI rendszerek bevezetésére és működtetésére.

3.3.6. Az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges

A GDPR 6. cikk (1) bekezdés alapján ez a jogalap nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre, így a vizsgálatától a témára tekintettel eltekinthetek.

3.4. Az MI és az érintetti jogok

Az érintetti jogokkal kapcsolatban előzetesen kiemelendő, hogy azok többsége gyakorol valamilyen hatást az adatkezelésre függetlenül a jog tartalmától, azonban a GDPR a tájékoztatáshoz / hozzáféréshez való jog és a tiltakozáshoz való joggal hozza kifejezetten kapcsolatba a profilalkotást és az automatizált döntéshozatalt.

3.4.1. Tájékoztatáshoz való jog és az érintett hozzáférési joga

A tájékoztatáshoz való jog és a hozzáféréshez való jog felfogható ugyanannak a kötelezettség proaktív és reaktív oldalának. Míg a GDPR 13-14. cikkei az érintettnek az adatgyűjtéskor nyújtandó tájékoztatásáról szólnak, addig a 15. cikk az érintett kérésére történő tájékoztatásról. A kettő e tekintetben különösebb eltérést nem mutat, a gyakorlatban a hozzáférési joghoz tud kapcsolódni betekintési vagy másolatkészítési igény is. Érdemes rögzíteni ezekkel a jogokkal kapcsolatban, hogy a GDPR speciális szabályokat állapít meg a profilalkotással és az automatizált döntéshozatallal kapcsolatos tájékoztatás tartalmára (ténye, alkalmazott logika, jelentősége az érintettre, várható következményei).[75] Aggályok terén említhető, hogy újra-hasznosított adatok esetén az ismeretlen érintett nem kap tájékoztatást, ennek megfelelően hozzáférési jogával sem élhet. Szintén nem egyértelmű, hogy az alkalmazott logikával kapcsolatos általános vagy

[73] Jóri András: i.m.
[74] GDPR 6. cikk (3) bekezdés
[75] GDPR 13. cikk (2) bekezdés f) pont, 14. cikk (2) bekezdés g) pont, 15. cikk (1) bekezdés h) pont

egyedi/személyre szabott tájékoztatás-e az elvárás.[76] A tájékoztatási kötelezettség, főként innovatív területeken, könnyen ütközhet az adatkezelő vélt vagy valós üzleti érdekeivel is,[77] így sokszor alapvető érdekellentét van az adatkezelő és az érintett között.[78]

3.4.2. Helyesbítéshez való jog

A jog a pontatlan vagy hiányos adatok kijavítására vonatkozik. Egy alapvető kérdés, hogy a pontatlansággal kapcsolatos kifogás csak a forrás adatok vonatkozásában merülhet fel vagy akár az MI rendszer által létrehozott új adatokkal szemben is.[79]

3.4.3. Törléshez való jog

Bizonyos esetekben[80] az adatkezelő köteles a kezelésében lévő személyes adatokat törölni. A törléssel érintett adathalmaz meghatározása okozza a legnagyobb értelmezési nehézséget, ugyanis nem egyértelmű, hogy a jog csak az input adatok, csak az output adatok, vagy esetlegesen mindkét adattípus esetén alkalmazható-e. Előbbi esetben elméletileg nem lehet akadálya, azonban a következménye fájdalmasnak bizonyulhat, hiszen a bemeneti adatok hiányában az MI rendszer pontossága nem ellenőrizhető. Az output adatokkal kapcsolatban azonban az sem egyértelmű, hogy azok megőrzik vagy elvesztik személyes adat jellegüket[81] (nyilván ennek a kérdésnek a megválaszolási nehézsége az MI típusától erősen függ). Ezen a ponton feltétlenül megjegyzendő, hogy a törléshez való joggal azonos aggályok merülnek fel a GDPR 20. cikkében jelölt adathordozhatósághoz való jog esetén is.

3.4.4. A tiltakozáshoz való jog

A tiltakozáshoz való jog szintén olyan, amely kifejezetten említ MI rendszerekkel rokon fogalmakat, amikor kimondja, hogy az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozhat személyes adatainak a 6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. A második fordulat szerint azonban, 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 az adatkezelés folytatható.[82] A tiltakozás általános

[76] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 56-57. o.
[77] Szőke Gergely László: *A közösségi oldalak szabályozási problémái.* In: Kis Kelemen Bence – Mohay Ágoston (Szerk.): *A technológiai fejlődés jogi kihívásai: Kézikönyv a jogalkotás és jogalkalmazás számára.* Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021. 106-107. o.
[78] Wachter, Sandra - Mittelstadt, Brent – Russel, Chris: i.m. 843. o.
[79] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 56-58 o.
[80] Személyes adatokra már nincs szükség, az érintett visszavonja a hozzájárulását és nincs más jogalap, az adatkezelés jogellenes, a törlést jog írja elő stb.
[81] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 57. o.
[82] GDPR 21. cikk (1) bekezdés

esetéhez képest többlet szabályokat találunk a direkt marketing, kutatási és statisztikai célú adatkezelések esetén. Ezeknek a jelentősége látható, ha a gyakorlatot vizsgáljuk, mivel mindkét típus rendszeresen alkalmaz MI rendszereket.[83] Előbbi esetében szigorúbb előírásokat találunk, mivel a tiltakozás feltétel nélküli, tehát nem vizsgálhatók kényszerítő erejű jogos okok a tiltakozás elutasítása érdekében. A GDPR közvetlen összefüggésbe hozza a direkt marketinggel a profilozást, így a tiltakozás szigorúbb esete alkalmazandó az ilyen célból létrehozott profilokkal szemben is.[84] A kutatási és statisztikai célok esetében megengedőbb szabály érvényesül, mivel azokkal szemben, amelyek közérdekű okból végzett feladat végrehajtása érdekében szükségesek a tiltakozás nem lehetséges. Az eredményes tiltakozás következménye egyébiránt azonos a törlési kérelemmel, az adatok nem kezelhetők tovább, így az aggályok is az ott leírtakkal azonosak.

3.5. Az MI és a GDPR 22. cikkének előírásai

Az alcímben szereplő jogszabályhely mutatja a legközelebbi kapcsolatot az MI rendszerekkel, mivel az automatizált döntéshozatalról, illetve az ehhez kapcsolódó profilalkotásról tartalmaz rendelkezéseket. Elöljáróban elmondható, hogy a 22. cikk előírásai nehezen megoldható feladatot adnak az MI rendszereket fejlesztő és alkalmazó szervezetek számára, rendkívül összetett és szigorú szabályrendszer miatt. A szigorúbb előírások indoka az algoritmizált folyamatok miatt megnövekedett kockázat a természetes személyek magánszférájára, emberi méltóságára és döntési-autonómiájára amelyek kétségkívül abszolút védendő értékek.[85] Lényeges, hogy kizárólag azon profilalkotás tartozik a 22. cikk hatálya alá, amelyen – mint automatizált adatkezelésen – valamilyen döntés alapul, tehát a profilalkotás továbbra sem tilos, csak annyiban, amennyiben a rá épülő automatizált döntés tilalmazott.[86] A teljesség érdekében a 22. cikk bekezdéseit külön vizsgálom.

3.5.1. Automatizált döntéshozatal tilalma

A 22. cikk (1) bekezdés szerint az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben[87] érintené. A GDPR szövegezése miatt nem egyértelmű, hogy ez a rendelkezés egy érintetti jogot vagy egy adatkezelői kötelezettséget hoz létre. Véleményem szerint az egyik oldalon felmerülő adatkezelői kötelezettség szükségképpen keletkeztetni fog a másik oldalon egy jogot, ami az előírások

[83] European Parliamentary Research Service, Scientific Foresight Unit (STOA): i.m. 57-59. o
[84] GDPR 21. cikk (2)-(6) bekezdések
[85] Zarsky, Tal: Transparent Predictions. *University of Illinois Law Review* ,2013/4. 1503–1570. o.
[86] Jóri András: i.m.
[87] 29. cikk szerinti munkacsoport WP251 sz. állásfoglalása alapján ilyen jelentős hatás lehet például egy szerződés megszűnése, határátlépés meghiúsulása, állampolgárság megszerzésének elmaradása.

kikényszeríthetőségét (a kötelezettség betartatását) szolgálja, így végeredményben mindkét értelmezés hasonlóan eredményre vezet.

3.5.2. Kivételek a tilalom alól

Tovább haladva a (2) bekezdés három kivételt említ az (1) bekezdés általános tilalma alól. Tehát lehetséges tisztán automatizált eszközökkel döntést hozni még akkor is, ha az az érintettre joghatással vagy hasonlóan jelentős hatással jár, amennyiben a kivételek valamelyike teljesül. A kivételek az alábbiak:

- a döntés az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
- a döntés meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- a döntés az érintett kifejezett hozzájárulásán alapul.

3.5.3. Védelmi intézkedések, garanciális szabályok

A Rendelet tovább fűzve a 22. cikk gondolatmenetét, a kivételszabály érvényesülése esetén további szigorú garanciális szabályokat állapít meg az érintett védelme érdekében, így az első vagy harmadik kivételszabály megvalósulása esetén az adatkezelő köteles megfelelő intézkedéseket tenni. A GDPR minimumszabályként említi az érintettnek azon jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

3.5.4. Különleges adatok helyzete az automatizált döntésekben

Egy utolsó szigorítást tartalmaz a 22. cikk (4) bekezdése, ami szerint a kivételszabályok esetén meghozott döntések nem alapulhatnak a személyes adatoknak a különleges kategóriáin.[88] Azonban a kivétel alkalmazásának tilalma alól is van kivétel azokban az esetekben, ha a különleges adatok kezelésére speciális felhatalmazást biztosító feltételek közül megvalósul vagy az érintett kifejezett hozzájárulását adta az adatkezeléshez[89] vagy a szóban forgó adatkezelés jelentős közérdek miatt szükséges,[90] továbbá az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

III. Összegzés

A fentiekben igyekeztem körképet adni elsősorban az MI rendszerek alkalmazásának aktuális trendjeiről, kitekintéssel a munkaügyi viszonyokra.

A GDPR előírásainak áttekintésével azt mondhatjuk, hogy a hatályos adatvédelmi jog nem tiltja az MI rendszerek fejlesztését, illetve alkalmazását és ez a

[88] GDPR 9. cikk (1) bekezdés
[89] GDPR 9. cikk (2) bekezdés a) pont
[90] GDPR 9. cikk (2) bekezdés g) pont

munkajogilag releváns területre is igaz. Léteznek továbbá olyan értelmezési módszerek, amelyeknek a követése esetén várhatóan az Európai Unió adatkezelői nem kerülnek versenyhátrányba Európán kívüli versenytársaikhoz képest. Sőt ideális esetben a mesterséges intelligencia fejlődése hosszútávon fenntarthatóbb módon valósulhat meg egy olyan környezetben, ami az innovatív gondolkodást az alapjogokat tiszteletben tartó formában támogatja.[91] Egyértelmű hiányosság jelenleg az egyértelmű jogi rendelkezések hiánya és a joggyakorlat kialakulatlansága, azonban ezen a közeljövő jogalkotása (e-Privacy rendelet,[92] DSA,[93] DMA,[94] MI-rendelet[95]) sokat javíthat. A tanulmány központi kérdéskörét alkotó aggályok tehát helyes hozzáállással és szilárd elhatározással tisztázhatók, a kockázatok mérsékelhetők, azonban szükség van további iránymutatásra a jogalkotó szervek és jogalkalmazó hatóságok részéről is. A munkaügyi viszonyokat vizsgálva megállapítható, hogy hatalmas az igény (és a szükség) az algoritmusok alkalmazására. Az ehhez szükséges szemléletváltás már elindult, de a gyakorlati megvalósítás tempója kellő mértékben nem gyorsul.

Az MI fejlesztési szakasza különösen kényesnek mutatkozik, ez a gyakorlatban valamelyest ellensúlyozásra kerülhet enyhítő intézkedések bevezetésével. Az alkalmazási szakasz alapvetően jobb lehetőségekkel indul, azonban a hatályos adatkezelési előírások betartása és a megmaradt, a folyamat szerves részét alkotó kockázatok kezelése valójában komoly kihívást jelent. Mindkét területnek meg kell küzdenie a magas kockázatú működés és a szigorú jogszabályi előírások terhével, azonban intézkedések bevezetése lényegesen jobb helyzetet idézhet elő. Nem kérdés, hogy e intézkedések költségnövelő tényezőként fognak megjelenni, és akár egyes innovációknak akadályát is jelenthetik. Ettől függetlenül a védendő értékek szem előtt tartásakor a megfelelő és helyes döntésnek mutatkozik ezeknek (vagy ehhez hasonló más) intézkedések betartása. Nem biztos ugyanis, hogy a rövidtávú gyors, de magas kockázatú fejlődés hosszú távon is megtartja előnyös tulajdonságait.

[91] Cohen, Julie E.: i.m. 2. o.
[92] Regulation on Privacy and Electronic Communications (COM(2017) 10 final)
[93] Digital Services Act (COM(2020) 825 final)
[94] Digital Markets Act (COM(2020) 842 final)
[95] Artificial Intelligence Act (COM(2021) 206 final)