DOI: 10.59851/imr.12.1.4 IN MEDIAS RES 2023/1. • 4, 53–70

A mesterséges intelligencia jogi szabályozásának aktuális kérdései az Európai Unióban

MEZEI KITTI*

A mesterséges intelligencia (MI) fejlesztésének biztosítania kell az emberközpontú és etikus működést, az átláthatóságot és az alapvető jogok tiszteletben tartását. Az MI nyilvánvaló előnyei mellett számos kockázatot is rejt magában, például az átláthatatlan döntéshozatalt. A termékekbe és szolgáltatásokba ágyazódó MI-vel kapcsolatos technológiák új biztonsági kockázatokat jelenthetnek a felhasználók számára. A tanulmány célja az MI jogi környezetének bemutatása és részletes elemzése az Európai Unióban, különös tekintettel az alapelvekre és az irányelvekre, valamint a jelenlegi és a lehetséges jövőbeli jogi keretre, az EU mesterséges intelligenciáról szóló rendelettervezetére.

Kulcsszavak: EU mesterséges intelligencia rendelettervezet, etikai alapelvek, kockázatalapú megközelítés, nagy kockázatú mesterséges intelligencia, megfelelőségértékelés

Current Issues in the Regulation of Artificial Intelligence in the European Union

The development of artificial intelligence (AI) must ensure human-centred and ethical operations, transparency and respect for fundamental rights. In addition to its obvious benefits, AI also entails a number of risks, such as opaque decision-making. Artificial intelligence technologies can pose new security risks for users when embedded in products and services. The aim of this paper is to present and analyse in detail the legal environment for AI in the European Union, with a particular focus on the principles and directives, as well as the current and possible future legal framework, the draft EU AI Act.

Keywords: EU Artificial Intelligence Act, ethical guidelines, risk-based approach, high-risk artificial intelligence, conformity assessment

* Tudományos munkatárs, Társadalomtudományi Kutatóközpont Jogtudományi Intézet; adjunktus, Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Üzleti Jog Tanszék.
A kutatás a Mesterséges Intelligencia Nemzeti Laboratórium és a 138965. számú NKFIH pályázat keretében, valamint az Európai Unió RRF-2.3.1-21-2022-00004 projekt, az Innovációs és Technológiai Minisztérium, a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal támogatásával valósult meg.
A kézirat lezárva: 2023. március 31.

1. Bevezetés

Az élet egyre több területén alkalmazzák a mesterséges intelligenciát, például javíthatja az egészségügyi ellátást,[1] előmozdíthatja a bűnüldöző hatóságok számára a bűnözés elleni hatékonyabb fellépést,[2] biztonságosabbá teheti a közlekedést,[3] vagy akár segíthet a csalás és a kiberbiztonsági fenyegetések észlelésében[4] stb. Korunk egyik legnagyobb kihívását jelenti, mind gazdasági, mind szabályozási szempontból. Ezt az is mutatja, hogy az Európai Unió (EU) Bizottsága 2020-ban közzétette a mesterséges intelligenciáról (MI) szóló fehér könyvet, amely az MI fejlesztéseinek és alkalmazásainak uniós szintű egyedi szabályozási alapja.[5] Ebben rögzítik, hogy mivel az MI jelentős hatást gyakorolhat társadalmunkra, szükséges, hogy kiépüljön az abba vetett bizalom, és kulcsfontosságú, hogy az MI-ágazat alapvető jogokon és értékeken alapuljon, így például az emberi méltóság és a magánélet védelmén. Az emberközpontú MI-nek olyan technológiává kell válnia, amelyben az emberek megbíznak, mert megfelel az emberi társadalmak alapjául szolgáló értékeknek.

A bizalom megteremtése, a kockázatok felmérése és a technológia szabályozása szempontjából meghatározó szerepe van a nem kötelező érvényű *soft law* megoldásoknak, például az etikai elveknek.[6] Ezek ugyanis beépülnek a szabályozásba, és már a jogszabályok kidolgozásának ideje alatt mérsékelhetik a kockázatokat. Az *ethics by design* olyan megközelítést takar, amellyel biztosítható, hogy megfelelően figyelembe veszik az etikai követelményeket az MI-rendszer vagy technika fejlesztése során. A célja az, hogy már a fejlesztés legkorábbi szakaszában foglalkozzanak az etikai kérdésekkel, ne csak utólag. Ráadásul ez a tendencia pozitív kulturális hatást fejthet ki, különösen a technológiai iparágban, ahol a piacvezetők inkább a szabályozás elé igyekeznek kerülni, mintsem lemaradni, termékeiket és szolgáltatásaikat úgy tervezik meg, hogy megfeleljenek a még csak tervezet formájában létező jogszabályoknak.

Az MI szabályozásának általános kialakítása kapcsán négy fő erkölcsi irányt kell kiemelni, amelyeket az MI-vel foglalkozó magas szintű szakértői csoport iránymutatásában olvashatunk:

– az emberi autonómia tiszteletben tartása (ne irányítsa vagy manipulálja az embert, ne veszélyeztesse a demokratikus folyamatokat),
– a károk megelőzése, ideértve a kár bekövetkezését eredményező nem kívánt külső behatásoknak való ellenállást,

---

1 Zorkóczy Miklós: A mesterséges intelligencia egészségügyi jogi és etikai dimenziói. *MTA Law Working Papers,* 2021/25., https://bit.ly/3Ni3axY.

2 Dobó Judit – Gyaraki Réka: A mesterséges intelligencia egyes felhasználási lehetőségei a rendvédelmi területeken. *Magyar Rendészet,* 2021/4., 67–81.

3 Kecskés Gábor: Az önvezető járművek lehetséges szerepe a fenntartható fejlődési célok elérésében. In Lévayné Fazekas Judit – Kecskés Gábor (szerk.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr, Universitas-Győr Nonprofit Kft., 2020, 155–175.

4 G. J. Priya – S. Saradha: Fraud Detection and Prevention Using Machine Learning Algorithms: A Review. 7th International Conference on Electrical Energy Systems (ICEES), 2021, 564–568.

5 Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése. Brüsszel, 2020.2.19, https://bit.ly/43n0eFU.

6 Lásd az etikai elvekkel szemben megfogalmazott kritikát, Mihály Héder: A Criticism of AI Ethics Guidelines. *Információs Társadalom,* 2020/4., 57–73.; Thilo Hagendorff: The Ethics of AI Ethics: An Evaluation of Guidelines. 30(1) *Minds & Machines* (2020) 99–120.

– méltányosság (az MI-rendszerek fejlesztésének és használatának méltányosnak kell lenniük),
– magyarázhatóság (a működés átláthatóságát jelenti[7] – a megbízható MI-rendszerek nyomon követhetők, döntéseik megmagyarázhatók; tájékoztatni kell a használókat, hogy MI-rendszerrel kerültek kapcsolatba, hogyan működik az MI-rendszer, milyen képességei vannak, milyen módon és megbízhatósággal használja a rendelkezésére bocsátott adatkészleteket).

További követelményként említhető az emberi cselekvőképesség és emberi felügyelet, a műszaki stabilitás és biztonság, az adatvédelem és -kezelés, a sokféleség, a megkülönböztetésmentesség és a méltányosság, a társadalmi és környezeti jólét, valamint az elszámoltathatóság.[8]

Az új MI-szabályozás arra ösztönöz, hogy már a fejlesztések kezdeti szakaszában foglalkozzanak a jogszabályi előírásokkal, az azoknak való megfeleléssel. Például a fehér könyv szerint az MI-rendszerekkel szemben elvárás, hogy beépített biztonsági és védelmi mechanizmusokkal rendelkezzenek, amelyek biztosítják, hogy a rendszer által végrehajtott bármely művelet igazolhatóan biztonságos az érintett személyek fizikai és mentális jóléte szempontjából. Az EU szabályozása is ebbe az irányba mutat több digitális szabályozási területen,[9] például az adatvédelem[10] és az algoritmikus kereskedés[11] szabályozása kapcsán.

---

7 Például ezzel összefüggésben elérhető már az IEEE P7001, egy új átláthatósági szabványtervezet, amely egyike az IEEE szabványügyi szövetség autonóm és intelligens rendszerek etikájával kapcsolatos globális kezdeményezéséből kialakuló P70XX „humán szabványok" sorozatának. A P7001 célja egy olyan szabvány létrehozása, amely „mérhető, tesztelhető átláthatósági szinteket határoz meg, hogy az autonóm rendszerek objektíven értékelhetők legyenek, és a megfelelőség szintjei meghatározhatók legyenek". A P7001 általános jellegű célja továbbá, hogy minden autonóm rendszerre alkalmazható legyen, beleértve a robotokat (autonóm járművek, segédrobotok, drónok, robotjátékok stb.), valamint a csak szoftveres MI-rendszereket, például az orvosi diagnosztika körében alkalmazott MI-t, a chatbotokat, az arcfelismerő rendszereket stb. A P7001 az érdekeltek öt különböző csoportját határozza meg, és az MI-rendszernek minden csoport számára átláthatónak kell lennie, különböző módon és okokból. Lásd erről részletesen Alan F. T. Winfield et al.: IEEE P7001: A Proposed Standard on Transparency. 8 *Frontiers in Robotics and AI* (2021).

8 High Level Expert Group on Artificial Intelligence: *Ethics Guidelines for Trustworthy AI.* Brüsszel, EU, 2019, 14–17.

9 Lásd Ronit Justo-Hanani: The Politics of Artificial Intelligence Regulation and Governance Reform in the European Union. 55 *Policy Sciences* (2022) 137–159.; Cristiano Codagnone – Giovanni Liva – Teresa Rodriguez de las Heras Ballel: *Identification and Assessment of Existing and Draft EU Legislation in the Digital Field*. Brüsszel, EU, 2022; az amerikai és uniós szabályozást összehasonlító elemzést lásd Jakob Mökander et al.: The US Algorithmic Accountability Act of 2022 vs. the EU Artificial Intelligence Act: What can They Learn from Each Other? 32(4) *Minds and Machines* (2022) 751–758.; lásd továbbá összehasonlításként a kínai MI-szabályozásról Huw Roberts et al.: The Chinese Approach to Artifcial Intelligence: An Analysis of Policy, Ethics, and Regulation. 36(1) *AI & Society* (2021) 59–77.

10 Beépített adatvédelem esetén a termékekbe és szolgáltatásokba már a fejlesztés legkorábbi szakaszától kezdve integrálni kell az adatvédelem garanciáit. Más szóval a vállalatoknak már az adatkezelési eljárások tervezési szakaszában, az adatfeldolgozás megkezdése előtt gondolniuk kell a biztonsági intézkedésekre. A beépített adatvédelemnek való megfelelőséget szolgálja például, ha a személyes adatokat álnevesítik vagy titkosítják.

11 A 2014/65/EU irányelv előírja a tagállamok számára annak biztosítását, hogy az algoritmikus kereskedési rendszerek ne teremtsenek rendezetlen kereskedési feltételeket a piacon, illetve ne járuljanak hozzá azokhoz, és hogy kezeljék azokat, amelyeket az ilyen algoritmikus kereskedési rendszerek mégis létrehoznak.

A technológiai gyártók hagyományosan utólag, a kockázat megvalósulása után vizsgálják termékeiket. Ha felelősséget állapítanak meg, intézkedéseket kell hozniuk folyamataik kijavítására és az esetleges károk megtérítésére. Ez a reaktív modell, amely mindig is nehezen tudott lépést tartani a technológiai fejlődéssel, kezd elavulttá válni. Ehelyett a jogalkotók arra ösztönzik a vállalatokat, hogy a „terméktanácsadók" köré *compliance* csapatokat alakítsanak ki, és már a kezdeti stádiumban számoljanak az adott termék által okozott károkkal és kockázatokkal, vagyis előzetes etikai és jogi kockázatértékelést végezzenek. Az ilyen szabályozás azonban rugalmas, és az adott vállalatra, termékre vagy szolgáltatásra igazítható előírásokat tartalmaz, például a „megfelelő technikai és szervezeti intézkedéseket". A beépített és az alapértelmezett adatvédelem kulcsfontosságú fogalom, és ma már a digitális szabályozás alapját képezik.[12]

Ezenkívül 2020-ban az Európai Parlament jelentést adott ki a Bizottságnak, amelyben ajánlásokat fogalmazott meg az MI-re vonatkozó polgári jogi felelősségrendszerrel kapcsolatban.[13] Erre válaszul 2022 szeptemberében a Bizottság egyfelől kezdeményezte a gyártók hibás termékekkel kapcsolatos objektív felelősségére vonatkozó szabályok korszerűsítését (az intelligens technológiától a gyógyszerekig).[14] A felülvizsgált szabályok célja, hogy jogbiztonságot teremtsenek a vállalkozások számára, megkönnyítve ezzel, hogy új és innovatív termékekbe fektethessenek be, továbbá gondoskodjanak a méltányos kártérítésről hibás – többek között digitális vagy felújított – termék okozta kár esetén. Másfelől a Bizottság most első alkalommal javaslatot nyújtott be az MI-re vonatkozó nemzeti felelősségi szabályok célzott összehangolására.[15] Az egységes szabályozás megkönnyítené az MI okozta károk károsultjai számára, hogy kártérítést kapjanak.[16]

A legfontosabb előrelépés az MI átfogó szabályozása terén, hogy 2021 áprilisában a Bizottság közzétette az MI-ről szóló rendelettervezetére *(Artificial Intelligence Act)* tett javaslatát,[17] amely fontos korlátozásokat tartalmaz az EU-ban vagy azzal összefüggésben használt MI-rendszerekre vonatkozóan.[18] A sajátos jellemzőkkel rendelkező (például a fekete doboz hatás miatt átláthatatlan, összetett, adatoktól függő vagy autonóm viselkedésű) MI alkalmazása hátrányosan érinthet az EU Alapjogi Chartájában rögzített számos alapvető jogot. Emiatt mind a hatóságok, mind az érintett személyek számára hiányozhatnak a megfelelő eszközök az adott algoritmikus döntéshozatal és a vonatkozó szabályok betartásának ellenőrzéséhez. Ezért a javas-

12 Osborne Clarke: *Legislators Worldwide Move to Adopt Regulation by Design,* https://bit.ly/3Tm4H6f.

13 Jelentés a Bizottságnak szóló ajánlásokkal a mesterséges intelligenciára vonatkozó polgári jogi felelősségrendszerrel kapcsolatban 2020.5.10. https://bit.ly/3WTLV9j.

14 Javaslat a termékfelelősségről szóló irányelv felülvizsgálatára. Brüsszel, 2022.9.28.

15 Irányelvjavaslat a szerződésen kívüli polgári jogi felelősségre vonatkozó szabályoknak a mesterséges intelligenciához való hozzáigazításáról. Brüsszel, 2022.9.28.

16 A termékekre és a mesterséges intelligenciára vonatkozó új felelősségi szabályok a fogyasztók védelme és az innováció előmozdítása érdekében, 2022. szeptember 28., https://bit.ly/3TngPUx.

17 Javaslat az Európai Parlament és a Tanács Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a Mesterséges Intelligenciáról Szóló Jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról. Brüsszel, 2021.4.21.

18 Megjegyzendő, hogy a rendelettervezetet más jelentős jogalkotási csomagokkal összefüggésben kell értelmezni, például a digitális szolgáltatásokról szóló rendelettel, a digitális piacokról szóló rendelettel és a digitális irányításról szóló rendelettel. Az első kettő főként a nagy kereskedelmi platformszolgáltatókat szabályozza, például a Google-t, az Amazont, a Facebookot és az Apple-t.

lat biztosítani kívánja ezen alapvető jogok magas szintű védelmét, és egyértelműen meghatározott, kockázatalapú megközelítéssel kívánja kezelni az esetleges veszélyek különböző forrásait. 2022. december 6-án az Európai Unió Tanácsa elfogadta közös álláspontját az MI rendelettervezetről, és számos ponton módosította a szövegét. A jelenlegi változatát legközelebb az Európai Parlamentnek kell elfogadnia. A tervek szerint a parlament 2023. március végéig szavaz a rendelettervezetről, majd várhatóan áprilisban kezdődnek meg a tagállamok, az Európai Parlament és a Bizottság közötti megbeszélések (ún. háromoldalú egyeztetések). Ha ez az ütemterv teljesül, akkor a jogszabályt 2023 végéig vagy 2024 elejéig kell elfogadni.

2. Az Európai Unió rendelettervezete a mesterséges intelligenciáról

2.1. A rendelettervezet hatálya és az MI-rendszer fogalmának meghatározása

Az MI-ről szóló uniós rendelettervezet a horizontális szabályozás minimumát célozza meg, és az EU-ban forgalomba hozott vagy használt valamennyi MI-rendszerre alkalmazandó. Az új szabályozás elsősorban az EU-ban vagy harmadik országban letelepedett, az EU piacán MI-rendszereket forgalomba hozó vagy az EU-ban üzembe helyező szolgáltatókra, valamint az EU-ban található MI-rendszerek felhasználóira vonatkozna.[19] A rendelet megkerülésének megakadályozása érdekében az új szabályok a harmadik országban található, MI-vel működő rendszerek szolgáltatóira és felhasználóira is vonatkoznának, amennyiben az e rendszerek által előállított kimenetet az EU-ban használják fel. A rendelettervezet azonban nem vonatkozik a kizárólag nemzetbiztonsági és katonai célokra fejlesztett vagy használt MI-alapú rendszerekre, harmadik országbeli hatóságokra, nemzetközi szervezetekre, valamint a bűnüldözési és igazságügyi együttműködésre vonatkozó nemzetközi megállapodások keretében MI-alapú rendszereket használó hatóságokra.[20] Az MI rendelet új változata rögzíti, hogy nem vonatkozik az olyan természetes személy felhasználók kötelezettségeire, akik a mesterséges intelligencia rendszereket tisztán személyes, nem szakmai tevékenységük során használják, kivéve az 52. cikket.

A Bizottság 2021 áprilisában egy technológiasemleges MI-definíciót javasolt a tervezet 3. cikk (1) bekezdésében, amely szerint az MI-rendszer

> olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek.

---

19 Lásd a 2. cikket. A rendelettervezet az uniós intézményekre, hivatalokra, szervekre és ügynökségekre is vonatkozna, amelyek az MI-rendszerek szolgáltatójaként vagy felhasználójaként járnak el.

20 A Tanács és az Európai Parlament egyes képviselői ezt kiterjesztenék azzal, hogy azokat az MI-rendszereket kizárnák a rendelet hatálya alól, amelyeknél nemzetbiztonsági kérdésekről van szó – ami lehetővé tenné (autokratikus) kormányok számára, hogy a „nemzetbiztonság" nevében és leple alatt biometrikus tömeges megfigyelést vagy társadalmi pontozást alkalmazzanak –, még akkor is, ha ezeket a rendelet tiltja.

Ennek megfelelően az „MI-rendszer" kifejezés olyan szoftveralapú technológiákra utalna, amelyek magukban foglalják a gépi tanulást, a logikai és tudásalapú rendszereket és a statisztikai megközelítéseket. Ez a tág meghatározás az önállóan vagy egy termék részeként használható MI-rendszereket is magában foglalja. Egy MI-rendszer tervezhető úgy, hogy különböző szintű autonómiával működjön, és önállóan vagy egy termék részeként legyen használható, függetlenül attól, hogy a rendszer fizikailag a termékbe van-e integrálva vagy sem. Az eredeti definíciót azonban módosították, a végleges szöveg az MI szűkebb meghatározást tartalmazza, mivel a tagállamok attól tartottak, hogy a tágabb definíció általában a szoftverekre is kiterjedne. A módosított meghatározás szerint a MI-rendszer

> olyan rendszer, amelyet úgy fejlesztenek, hogy az autonóm módon és önállóan működjön, valamint a gépi és/vagy az ember által szolgáltatott adatok és bemenetek alapján gépi tanulás és/vagy logikai és tudásalapú megközelítések alkalmazásával következtetéseket von le meghatározott célkitűzések eléréséhez, és a rendszer által generált eredményeket, például tartalmat (generatív MI-rendszerek), előrejelzéseket, ajánlásokat vagy döntéseket alkot, amelyek hatással vannak az MI-rendszer környezetére.

A (6) preambulumbekezdés szerint az MI-rendszer autonómiájának fogalma arra vonatkozik, hogy egy ilyen rendszer milyen mértékben működik emberi közreműködés nélkül. Ezenkívül bevezették külön a generatív MI-rendszer fogalmát:

> olyan MI-rendszer, amelyet – függetlenül attól, hogy hogyan hozták forgalomba vagy helyezték üzembe, beleértve a nyílt forráskódú szoftvert is – a szolgáltató olyan általánosan alkalmazható funkciók ellátására szán, mint például kép- és beszédfelismerés, hang- és videógenerálás, mintafelismerés, kérdésmegoldás, fordítás és egyéb; a generatív MI-rendszer többféle összefüggésben használható és többféle más MI-rendszerbe integrálható.

A rendelettervezet célja továbbá, hogy a jövőre nézve biztos legyen *(future proof),* és lefedje a jelenlegi és a jövőbeli MI-technológiai fejlesztéseket. Ennek érdekében a Bizottság – felhatalmazáson alapuló jogi aktusok elfogadásával (4. cikk) – kiegészítené az I. mellékletben szereplő listát az MI fejlesztéséhez használt új megközelítésekkel és technikákkal, amint azok megjelennek. A 3. cikk a fogalommeghatározások hosszú listáját is tartalmazza, beleértve az MI-rendszerek – állami és magánszervezetekre egyaránt kiterjedő – szolgáltatója, felhasználója, valamint az importőr, a forgalmazó és az üzemeltető, továbbá az érzelemfelismerés és a biometrikus kategorizálás fogalmát.

2.2. A kockázatalapú megközelítés

Az MI alkalmazása, annak sajátos jellemzői miatt, hátrányosan érinthet számos alapvető jogot és a felhasználók biztonságát is. Ennek kezelése érdekében a rendelettervezet kockázatalapú megközelítést alkalmaz, amelynek értelmében az MI-alkalmazásokat kockázati osztályokba so-

rolják, és a jogi fellépést a konkrét kockázati szinthez igazítják.[21] E célból különbséget tesz az elfogadhatatlan, a nagy és a mérsékelt kockázatot jelentő MI-rendszerek között. E megközelítés szerint az MI-alkalmazásokat csak a konkrét kockázati szintek kezeléséhez feltétlenül szükséges mértékben kívánják szabályozni.

2.2.1. A tiltott kategóriába eső MI-rendszerek

A tervezet megkülönböztet teljesen tiltott kategóriát (II. cím) – ebbe tartozik az arcfelismerő programok[22] (kivételt engedő)[23] tiltása közterületen, a tudatalatti manipuláció, a tömeges megfigyelés vagy a (Kínában használthoz hasonló) társadalmi pontrendszer[24] jogellenességének rögzítése. A rendelettervezet új szövegében a társadalmi pontrendszer alkalmazásának tilalmát kiterjesztették a közszférán túl a privát szférára is. Ez azt hivatott biztosítani, hogy az állami szférában ne kerülhessék meg e rendelkezést, ugyanis a magánszféra szereplőivel szerződést köthetnének arra vonatkozóan, hogy az állami szervek számára társadalmi pontozást végezzenek. Ezenkívül minden olyan MI-rendszert tiltanak, amely egyértelműen veszélyezteti az emberek biztonságát, megélhetését és jogait, a kormányok által végzett társadalmi pontozástól kezdve a veszélyes viselkedésre ösztönző hangasszisztenst használó játékokig. Ezek közül a tudatalatti manipulációt érte a legtöbb kritika, mert a tervezet nem nyújt pontos meghatározást arra vonatkozóan, hogy mit ért ez alatt, milyen esetek tartozhatnak ebbe a kategóriába. A szakirodalom szerint általában olyan érzékszervi ingerekről van szó, amelyeket a fogyasztók nem tudnak tudatosan érzékelni, például az 50 milliszekundumnál rövidebb ideig megjelenő vizuális ingereket. Az MI legtöbb alkalmazása azonban nem lesz tudatalatti, mivel a felhasználók tudatosan érzékelik. Így a rendelettervezet jelenlegi formájában még mindig lehetővé teszi az MI-alapú manipuláció számos formáját.[25]

---

21 Lásd bővebben Tobias Mahler: Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal. In *Nordic Yearbook of Law and Informatics,* 2021, 245–276.

22 Lásd bővebben az arcfelismerő programok szabályozásáról az EU-ban Tambiama Madiega – Hendrik Mildebrath: *Regulating Facial Recognition in the EU.* Brüsszel, EU, 2021.

23 Az MI-rendszerek természetes személyek „valós idejű" távoli biometrikus azonosítására, a nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használata szükségszerűen magában foglalja biometrikus adatok feldolgozását. A rendelettervezetnek azokat az EUMSZ 16. cikkén alapuló szabályait, amelyek – bizonyos kivételekre is figyelemmel – tiltják az ilyen használatot, *lex specialis*ként kell alkalmazni az (EU) 2016/680 irányelv 10. cikkében foglalt, a biometrikus adatok kezelésére vonatkozó szabályok tekintetében, ennélfogva ezek kimerítően szabályozzák az ilyen használatot és az érintett biometrikus adatok kezelését.

24 Lásd Nicolas Kayser-Bril: Personal Scoring in the EU: Not Quite *Black Mirror* Yet, at Least If You're Rich. *Algorithm Watch,* 2019, https://bit.ly/3MAQBvM.

25 A Future of Life Institute szemléletes példája szerint képzeljük el, hogy van egy szenzorokkal felszerelt vizespalackunk, amely adatokat küld vissza a telefonunkon lévő egészségügyi alkalmazásba. Ha már régen nem töltöttük meg a palackot, egy algoritmus arra következtethet, hogy szomjasak vagyunk – még ha ezt nem is vesszük észre –, ezért egy cukros ital reklámját jeleníti meg nekünk. Ez az ital megvásárlása felé terelne minket, és akkor célozna meg, amikor kiszolgáltatott állapotban vagyunk. Ez a manipuláció azonban nem számítana tudatalattinak, amíg tudatosan érzékeljük a reklámot. Az MI manipulációjának ez a konkrét példája viszonylag ártalmatlannak tűnhet, de ez nem mindig lesz ilyen. Risto Uuk: *Manipulation and the AI Act.* Future of Life Institute (2022), https://bit.ly/3qzTqpO; bővebben még erről Matija Franklin et al.: Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings* 35 (2022); Suzanne

2.2.2. A kevésbé kockázatos MI-rendszerek

A tervezet meghatározza a nagy kockázatú MI-alkalmazásokat (III. cím), amelyekre kötelező szabályokat is alkot, és a kevésbé kockázatos (IV. cím), de valamilyen szempontból még mindig kiemelt figyelmet érdemlő egyéb alkalmazásokat, amelyeket az átláthatóságot erősítő rendelkezésekkel támogatva kezel. Ezeket a szabályokat az 52. cikk tartalmazza, amelynek értelmében az MI-nek mindig tájékoztatnia kell az embert, hogy MI-vel áll szemben. Az érzelmek felismerésére képes rendszerek felhasználóinak tájékoztatniuk kell az érintetteket, a *deepfake* videókat fel kell címkézni, tudatni kell, hogy gépi eszközökkel hamisított mozgóképről van szó. Ezek a kategóriák önmagukban nem minősülnek sem tiltottnak, sem nagy kockázatúnak.[26] Érdekesség, hogy előzetesen a bűnüldöző szervek által használt, a *deepfake* kiszűrésére szolgáló eszközök nagy kockázatúnak minősültek, míg általában a *deepfake* tartalmak az alacsony kockázatú kategóriába tartoznak, de ez az utóbbi módosítás eredményeképpen megváltozott, ugyanis a következő nagy kockázatú felhasználási eseteket törölték: a *deepfake* észlelését a bűnüldöző szervek által, a bűnügyi analitikát, valamint az úti okmányok hitelességének ellenőrzését. Azonban a rendelettervezet szerint ez a címkézési kötelezettség nem vonatkozik a bűnüldözésre. Ez azt jelenti, hogy amikor egyes bűnüldöző hatóságok *deepfake*-et használnak, azt nem kell feltüntetniük [52. cikk (3) bekezdés].[27]

A Tanács egy másik érdekes módosítása a 52. cikk (3) bekezdésében található. Ez a bekezdés most már kifejezetten kimondja, hogy az MI által generált (audiovizuális) kimenetnek nem kell felfednie ezt a jelleget, „ha a tartalom nyilvánvalóan kreatív, szatirikus, művészi vagy fikciós mű vagy program része". Ez azt jelenti, hogy például a Dall-E-t használó művészeknek nem kell jelezniük, hogy MI-eszközöket használnak. Ez szerzői jogi szempontból nagyon fontos, mivel az MI által létrehozott művészet a jelenlegi európai szerzői jogi rendszerben nem élvezhet ilyen védelmet. Ezért felül kell vizsgálni, hogy megfelelő-e ez a kizárás.

A biometrikus kategorizálási rendszerek – amelyek biometrikusan csoportosítják az egyéneket meghatározott kategóriák szerint (nem, kor, hajszín, szemszín, tetoválás, etnikai származás, szexuális vagy politikai irányultság) biometrikus adataik alapján – vagy az érzelemfelismerő rendszerek, amelyek a 3. cikk (34) bekezdése szerint az egyének érzelmi állapotának a biometrikus adatok alapján történő értékelésére vagy következtetésére irányulnak, nem tiltottak, és nem szerepelnek a nagy kockázatú MI-rendszerek listáján. Következésképpen a mérsé-

---

Vergnolle: Identifying Harm in Manipulative Artificial Intelligence Practices. *Internet Policy Review,* 2021, https://bit.ly/3Clyg1e; Phillip Hacker: Manipulation by Algorithms: Exploring the Traingle of Unfair Commercial Practice, Data Protection and Privacy Law. *European Law Journal,* 2021, 1–34.

26 Érdemes említést tenni egy olyan hazai esetről, amelyben a Nemzeti Adatvédelmi és Információszabadság Hatóság első alkalommal szabott ki büntetést az MI jogszerűtlen használata miatt, 250 millió forintra bírságolva egy pénzintézetet. A hatóság beszámolója szerint egy bank MI-vel vezérelt szoftveres megoldást alkalmazott az ügyfelek érzelmi állapotának automatizált feldolgozására. A beszédjel-felismerő és -értékelő rendszer az ügyfelek hangulati állapota alapján határozta meg, mely ügyfeleket szükséges visszahívni. A bank az alkalmazást a panasz és az ügyfélelvándorlás megelőzése érdekében üzemeltette. A hatóság utasította a bankot az érzelmi állapotok elemzésének abbahagyására, mivel az számos ponton sérti az általános adatvédelmi rendeletet.

27 Ilina Georgieva – Tjerk Timan – Marissa Hoekstra: *Regulatory Divergences in the Draft AI Act. Differences in Public and Private Sector Obligations.* Brüsszel, EU, 2022, 14–21.

kelt kockázatot jelentő MI-rendszerek kategóriájába tartoznak, és ezért rájuk vonatkoznak az 52. cikk (2) bekezdése szerinti rendelkezések mind a köz-, mind a magánszféra szereplői számára, a bűnüldöző szervek kivételével. Az újonnan hozzáadott 52. cikk (2a) bekezdés hangsúlyozza az érzelemfelismerő rendszer felhasználóinak azon kötelezettségét, hogy tájékoztassák a természetes személyeket, ha ilyen rendszerrel érintkeznek. Végül a tervezet az egyik kategóriába sem eső MI-alkalmazásokat a magatartási kódexekre, vagyis az önszabályozásra bízza.[28]

2.2.3. A nagy kockázatú MI-rendszerek

A legérdekesebb számunkra a nagy kockázatú MI-k szabályozása, mert az új szabályozás legtöbb rendelkezése e kockázati kategória köré épül. Nagy kockázatúnak akkor minősül egy MI-rendszer, ha vagy biztonsági komponense egy egyébként is szorosan szabályozott termékcsoportnak (ezeket a II. melléklet sorolja fel a játékoktól a vízi járműveken keresztül az orvosi műszerekig), vagy azért, mert olyan területen alkalmazzák, amely az emberi jogokat különösen érinti. Ez utóbbi melléklet nyolc területen kéttucatnyi konkrét alkalmazást sorol fel, például a természetes személyek biometrikus azonosítását, kritikus infrastruktúrák (közlekedés, gáz, víz, villanyellátás) vezérlését végző MI-k, és még néhány, különösen az amerikai szakirodalomból ismert területeken „tevékenykedő" MI (így a munkaerő-felvétel, egyetemi felvétel, hitelbírálat és a bírói munkához adott tanácsok területén működő alkalmazások).[29] A biztonsági komponens rendszertől eltekintve az MI-rendszerek tehát akkor minősülnek nagy kockázatúnak, ha szerepelnek a III. melléklet listáján, „kivéve, ha a rendszer kimenete a meghozandó intézkedés vagy döntés tekintetében pusztán kiegészítő jellegű" (a rendelettervezet módosított 6. cikkének 3. bekezdése értelmében). Az utóbbi részt a Tanács a végleges változatban egészítette ki. A (32) preambulumbekezdés a következőképpen pontosítja a „pusztán kiegészítő" kifejezést: „a mesterséges intelligencia rendszer kimenete csak elhanyagolható vagy csekély jelentőséggel bír az emberi cselekvés vagy döntés szempontjából." Annak paramétereit, hogy mi minősül „tisztán kiegészítőnek", a Bizottság fogja meghatározni a végrehajtási jogi aktuson keresztül.

A rendelettervezet például rögzíti, hogy nagy kockázatúnak kell tekinteni azokat az MI-rendszereket, amelyeket a foglalkoztatás, a munkavállalók irányítása és az önfoglalkoztatáshoz való hozzáférés, különösen személyek felvétele és kiválasztása, az előléptetéssel és felmentéssel kapcsolatos döntések meghozatala, valamint a munkával kapcsolatos szerződéses jogviszonyban lévő személyek részére történő feladatkiosztás, továbbá az ilyen személyek nyomon követése vagy értékelése során használnak, mivel ezek a rendszerek érzékelhetően befolyásolhatják e személyek jövőbeli karrierlehetőségeit és megélhetését.

A bűnüldöző hatóságoknak az MI-rendszerek bizonyos használatával járó fellépéseit az erőviszonyok jelentős mértékű kiegyensúlyozatlansága jellemzi, és egy természetes személy megfigyeléséhez, letartóztatásához vagy szabadságának elvonásához, valamint az Alapjogi Chartában garantált alapvető jogokra gyakorolt egyéb kedvezőtlen hatásokhoz vezethetnek. Különösen akkor, ha az MI-rendszert nem tanítják jó minőségű adatokkal, nem felel meg a

[28] Ződi Zsolt: Az Európai Bizottság Mesterséges Intelligencia Kódexének tervezete. *Gazdaság és Jog,* 2021/5., 1–3.

[29] Ződi Zsolt: A mesterséges intelligencia szabályozásának dilemmái. *ITKI blog,* 2020. augusztus 24., https://bit.ly/3jTb5lW.

pontosságával vagy stabilitásával szemben támasztott megfelelő követelményeknek, vagy a forgalomba hozatalt vagy a más módon történő üzembe helyezést megelőzően nem megfelelően tervezték és tesztelték, akkor e rendszer diszkriminatív vagy más tekintetben tisztességtelen vagy igazságtalan módon választhat ki embereket. Akadályozhatja továbbá a fontos alapvető eljárási jogoknak – például a hatékony jogorvoslathoz, a tisztességes eljáráshoz, a védelemhez való jognak és az ártatlanság vélelmének – az érvényre juttatását, különösen akkor, ha az ilyen MI-rendszerek nem eléggé átláthatók, megmagyarázhatók és dokumentálhatók.[30]

A migrációkezelésben, a menekültügyben és a határigazgatásban használt MI-rendszerek[31] olyan embereket érintenek, akik gyakran különösen kiszolgáltatott helyzetben vannak, és akiknek az életét befolyásolja az illetékes hatóságok intézkedéseinek kimenetele. Az ilyen összefüggésben használt MI-rendszerek pontossága, megkülönböztetésmentes jellege és átláthatósága ezért különösen fontos az érintett személyek alapvető jogai, nevezetesen a szabad mozgáshoz, a megkülönböztetésmentességhez, a magánélet és a személyes adatok védelméhez, a nemzetközi védelemhez és a megfelelő ügyintézéshez való jogaik tiszteletben tartásának biztosítása szempontjából. Az igazságszolgáltatásra és a demokratikus folyamatok irányítására szánt egyes MI-rendszereket nagy kockázatúnak kell tekinteni, figyelembe véve a demokráciára, a jogállamiságra, az egyéni szabadságokra, valamint a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogra gyakorolt jelentős hatásukat.

Különösen az esetleges torzítások, hibák és az átláthatatlanság kockázatának kezelése érdekében indokolt nagy kockázatúnak minősíteni azokat az MI-rendszereket, amelyek célja, hogy segítsék az igazságügyi hatóságokat a ténybeli és jogi elemek kutatásában és értelmezésében, valamint a jog konkrét tényekre történő alkalmazásában. Ez a minősítés azonban nem terjedhet ki azokra az MI-rendszerekre, amelyeket olyan tisztán járulékos adminisztratív tevékenységekre szánnak, amelyek az egyedi esetekben nem befolyásolják a tényleges igazságszolgáltatást; ilyen tevékenység például a bírósági határozatok, dokumentumok vagy adatok anonimizálása vagy álnevesítése, a személyzet közötti kommunikáció, az adminisztratív feladatok ellátása vagy a források elosztása.

A jegyzék a következő területekkel egészül ki a nagy kockázatú rendszerek esetében: kritikus digitális infrastruktúra, életbiztosítás és egészségbiztosítás. A végrehajtáskor a Bizottság (meghatározott feltételek mellett) hozzáadhat és törölhet nagy kockázatú felhasználási eseteket.

A nagy kockázatú MI-vel szemben támasztott követelmények a rendeletben következők (2. fejezet): mindig kockázatértékelési rendszereket kell létrehozni, bevezetni, dokumentálni és fenntartani (9. cikk). Megfelelő adatmenedzsment *(data governance)* rendszerekkel kell együtt működtetni, valamint a tanító, validáló és tesztelő adatoknak „tisztának" kell lenniük (10. cikk). A nagy kockázatú MI-khez részletes dokumentációt kell csatolni, az eseményeket naplózó rendszereket kell társítani (11–12. cikk). Az ilyen típusú rendszereknek átláthatóan kell működniük, valamint mindig meg kell maradnia az emberi felügyeletnek és beavatkozási lehetőségnek (13–14. cikk). Ezenkívül meg kell felelnie a pontosság, a robosztusság és a

30 Lásd bővebben Karsai Krisztina: A mesterséges intelligencia szabályozásának európai tervezete, avagy algoritmusok térnyerésének előjelei a (büntető) igazságszolgáltatásban. *Forum: Acta Juridica et Politica,* 2021/3., 189–196.

31 Lásd Costica Dumbrava: *Artificial Intelligence at EU Borders.* Brüsszel, European Parliamentary Research Service, 2021.

kiberbiztonság követelményeinek (15. cikk). Fontos, hogy e követelmények többségét be kell építeni a nagy kockázatú MI-rendszer tervezésébe.

A szolgáltató által elkészítendő műszaki dokumentáción kívül a többi követelményt már az MI-rendszer tervezésének és fejlesztésének legkorábbi szakaszában figyelembe kell venni. Még ha nem is a szolgáltató a rendszer tervezője/fejlesztője, akkor is gondoskodnia kell arról, hogy a 2. fejezet szerinti követelmények beépüljenek a rendszerbe a megfelelőségi státusz elérése érdekében. A rendelettervezet a nagy kockázatú MI-rendszerekre vonatkozó követelményeknek való megfelelés vélelmét is megállapítja, amennyiben a nagy kockázatú MI-rendszer megfelel a vonatkozó harmonizált szabványoknak. Amennyiben nem léteznek harmonizált szabványok vagy azok nem elegendők, az Európai Bizottság közös előírásokat fogadhat el, és az azoknak való megfelelés szintén ilyen megfelelési vélelemhez vezet. A rendelettervezet bevezeti a „megfelelőségértékelést" *(conformity assessment),* amely annak ellenőrzésére szolgál, hogy egy adott MI-rendszer vonatkozásában teljesülnek-e a rendelet III. cím 2. fejezetében meghatározott követelmények.

Az összes nagy kockázatú MI-rendszerre egy sor új megfelelési szabály vonatkozna, többek között az előzetes megfelelőségértékeléssel összefüggő követelmények *(ex-ante conformity assessment)*, amelyek szerint a nagy kockázatú MI-rendszerek szolgáltatóinak a forgalomba hozatal vagy üzembe helyezés előtt regisztrálniuk kell rendszereiket a Bizottság által kezelt, az egész EU-ra kiterjedő adatbázisban. A meglévő termékbiztonsági jogszabályok hatálya alá tartozó MI-vel kapcsolatos termékek és szolgáltatások a már meglévő, harmadik fél által alkalmazott megfelelőségi keretrendszerek hatálya alá tartoznak (például az orvostechnikai eszközök esetében). A jelenleg az uniós jogszabályok hatálya alá nem tartozó MI-rendszerek szolgáltatóinak saját megfelelőségértékelést (önértékelést) kell végezniük, amely igazolja, hogy megfelelnek a nagy kockázatú mesterséges intelligencia rendszerekre vonatkozó új követelményeknek, és használhatják a CE jelölést. Csak a távoli biometrikus azonosításra használt, nagy kockázatú MI-alapú rendszerek esetében lenne szükség harmadik fél, „bejelentett szervezet" általi megfelelőségértékelésre. A harmadik fél által végzett megfelelőségértékelésnek megvannak a maga előnyei, és kérdésként felmerül, megfelelő-e, hogy csak az MI-rendszerek egy nagyon szűk csoportjára korlátozzák ezt.

A nagy kockázatú MI-t alkalmazó rendszerek szolgáltatóinak, importőreinek, forgalmazóinak és felhasználóinak számos kötelezettséget kellene teljesíteniük. Az EU-n kívül letelepedett szolgáltatóknak ki kell jelölniük egy meghatalmazott képviselőt az EU-ban, aki (többek között) biztosítja a megfelelőségértékelést, létrehoz egy forgalomba hozatal utáni felügyeleti rendszert, és szükség esetén korrekciós intézkedéseket hoz. Felmerül a kérdés, hogy mikor kell elvégezni a megfelelőségértékelést. Az MI-rendszer uniós piacon történő forgalomba hozatala előtt kell elvégezni, ami azt jelenti, hogy a rendszer hozzáférhetővé tétele (azaz a forgalmazása vagy használatra történő átadása), az üzembe helyezése előtt, tehát még azt megelőzően, hogy első alkalommal sor kerülne a rendszer uniós piaci használatára akár a rendszer felhasználója által, akár a szolgáltató saját használatára. Ezenkívül új megfelelőségértékelést kell végezni, ha a nagy kockázatot jelentő MI-vel rendelkező rendszert jelentősen módosítják, azaz ha a változás befolyásolja a rendszer megfelelését a rendelettervezet követelményeinek, vagy ha az MI-rendszer rendeltetésének módosítását eredményezi. Nincs szükség új megfelelőségi eljárásra azonban akkor, ha a nagy kockázatú MI-rendszer a forgalomba hozatal vagy üzembe helyezés után tovább tanul, amennyiben ezeket a változásokat az megfelelőségértékelés időpontjában előre meghatározzák

és a kezdeti műszaki dokumentációban leírják. A végleges szöveg az MI fejlesztésének és alkalmazásának összetett értékláncát megértve pontosítja és kiigazítja a nagy kockázatú rendszerekre vonatkozó követelményeket. Ez a következőket tartalmazza: az adatok minősége; a műszaki dokumentáció, amellyel a kis- és középvállalkozásoknak rendelkezniük kell annak bizonyítására, hogy a nagy kockázatot jelentő rendszereik megfelelők; a felelősség kérdését rendezi az MI életciklusának különböző szakaszaiban. A szöveg tisztázza a rendelettervezet szerinti felelősségek és más jogszabályok kapcsolatát, például az adatvédelmi és az ágazati jogszabályok, köztük a pénzügyi szolgáltatásokra vonatkozó szabályozás alapján már meglévő felelősségek közötti kapcsolatot.

A tervezet szigorú feltételek mellett (lásd a 47. cikket) bevezeti annak lehetőségét, hogy „a közbiztonsággal, a személyek életének és egészségének védelmével, a környezetvédelemmel, valamint a kulcsfontosságú ipari és infrastrukturális eszközök védelmével kapcsolatos kivételes okokból" el lehessen térni a hitelesítés elvégzésére vonatkozó kötelezettségtől. A megfelelőségeljárást elsősorban a nagy kockázatú MI-rendszer szolgáltatója végzi, de bizonyos helyzetekben a termék gyártója, a forgalmazó, az importőr vagy harmadik fél is elvégezheti.

Ezzel összefüggésben fontos áttekinteni, hogy a nagy kockázatú MI-rendszerek piacra lépése előtt melyik négy lépést kell elvégezni. Megjegyzendő, hogy ezek a lépések az ilyen MI-rendszerek összetevőire is vonatkoznak. Az első lépés a nagy kockázatú MI-rendszer kifejlesztése, lehetőleg előzetes belső hatásvizsgálatok és magatartási kódexek segítségével, amelyeket inkluzív, multidiszciplináris csoportok felügyelnek. A második lépés, hogy az MI-rendszernek jóváhagyott megfelelőségértékelésen kell átesnie, és életciklusa során folyamatosan meg kell felelnie a rendelettervezetben meghatározott követelményeknek. Bizonyos rendszerek esetében a megfelelőségértékelés ellenőrzésébe bejelentett külső szervezetet vonnak be. Ez a dinamikus folyamat biztosítja a teljesítményértékelést, a nyomon követést és a hitelesítést. A nagy kockázatú MI-rendszer módosításakor a második lépést meg kell ismételni. A harmadik lépés az önálló, nagy kockázatú MI-rendszert jelző rendszer nyilvántartásba vétele egy erre a célra létrehozott uniós adatbázisban . Negyedik lépésként alá kell írni egy megfelelőségi nyilatkozatot (48. cikk), és a nagy kockázatú MI-rendszeren fel kell tüntetni a CE jelölést *(Conformité Européenne)* (49. cikk).[32] E folyamat végén az MI-rendszer készen áll az európai piacra való belépésre, de ezzel még nem zárul le teljesen a folyamat. A Bizottság elképzelése szerint, miután a nagy kockázatú MI-rendszer megkapta a piaci engedélyt, onnantól az uniós és tagállami szintű hatóságok felelősek a piacfelügyeletért, a végfelhasználók biztosítják a felügyeletet, a szolgáltatók pedig a forgalomba hozatal utáni felügyeleti rendszerről gondoskodnak.

A szolgáltatók és a felhasználók a súlyos incidenseket és a hibás működést is jelenteni fogják. Más szóval, folyamatos előzetes és utólagos nyomon követés valósul meg. A rendelettervezet ugyanis előírja a forgalomba hozatal utáni nyomon követést *(post-market monitoring),* ami azt jelenti, hogy a nagy kockázatú MI-rendszerek szolgáltatóinak megfelelő forgalomba hozatal utáni felügyeleti rendszert kell létrehozniuk és dokumentálniuk kell a szabályozási követelmé-

[32] A CE jelölést a nagy kockázatú MI-rendszerek esetében jól láthatóan, olvashatóan és eltávolíthatatlan módon kell elhelyezni. Ha a nagy kockázatú MI-rendszer jellege miatt ez nem lehetséges vagy nem indokolt, a jelölést a csomagoláson vagy a kísérő dokumentáción kell feltüntetni. A CE jelölésre a 765/2008/EK rendelet 30. cikkében meghatározott általános elvek vonatkoznak.

nyeknek való megfelelést. A súlyos eseményeket és működési zavarokat jelenteniük kell azon tagállam piacfelügyeleti hatóságának, ahol az esemény vagy a kapcsolódó alapjogsértés történt. A piacfelügyeleti hatóságoknak fel kell szólítaniuk az érintett üzemeltetőket, hogy hozzák meg a megfelelő intézkedéseket, vagy akár vonják vissza az MI-rendszert, ha az megsérti a rendeletet vagy ha az – bár megfelel a rendeletnek – kockázatot jelent az egészségre, a biztonságra, az emberi jogokra vagy a közérdekre.

Végül érdemes foglalkozni az MI-rendszerek használatakor, különösen az algoritmikus döntéshozatal esetén az egyik legnagyobb veszélynek kitett alapvető joggal: az esélyegyenlőséghez való joggal és a diszkrimináció tilalmával. Ezeket leginkább az MI által alkalmazott vagy a betanítása során felhasznált adatkészlet hiányossága, hibája vagy a rendszerben rejlő elfogultság veszélyezteti. Az algoritmikus döntéshozatal előítéletessége, amit az adatkészlet ilyen problémái okozhatnak, anélkül is jogsértéshez vezet, hogy szándékosság vagy emberi tudatosság állna mögötte. Az MI döntéshozatala diszkriminatív eredményeket is hozhat, ha a rendszer diszkriminatív adatokból tanul, ezért a rendelettervezet szigorú követelményeket támaszt a tanítóadatokkal szemben.[33] Az adat és a jól kiválasztott tanítóadat (a példák) kulcsfontosságúvá válik. A kód előállítójának felelőssége pedig annyiban változik, hogy nem a kódolásért (a hibátlan programért), hanem elsősorban az adat minőségéért és a példák helyes kiválasztásáért kell felelnie.[34]

Érdemes közelebbről megvizsgálni a tanítóadatokkal kapcsolatos 10. cikkben foglalt, a tanítóadatokra vonatkozó irányítási rendszert meghatározó rendelkezést, amely átfogó követelményeket tartalmaz az ilyen adathalmazok teljes életciklusára vonatkozóan, amikor azokat nagy kockázatú MI-alkalmazások tanítására használják. A rendelettervezet a nagy kockázatú rendszerekre vonatkozó konkrét minőségi kritériumok három fontos csoportjának meghatározásával folytatódik. Először is, a 10. cikk (3) bekezdése szerint a tanítóadatoknak „relevánsnak, reprezentatívnak, hibamentesnek és teljesnek" kell lenniük, ami az informatikai szakirodalomban foglalt számos adatminőségi követelményt tükrözi, de ezeket részletesen nem fejti ki. Másodszor, a tanítóadatoknak megfelelő statisztikai tulajdonságokkal kell rendelkezniük, azon személyek vagy személyek azon csoportjaira is kiterjedően, akikre vagy amelyekre a nagy kockázatú MI-rendszert alkalmazni kívánják. A statisztikai megfelelőségnek azonban minden kellően megkülönböztethető csoport tekintetében teljesülnie kell, függetlenül attól, hogy a védett tulajdonságok által meghatározott vagy nem meghatározott csoportról van-e szó, ami a rendelkezést egyszerre tágítja (gondoljunk például a különböző társadalmi-gazdasági csoportokra) és teszi homályossá. Minden csoport esetében megfelelő statisztikai tulajdonságokat ír elő, anélkül azonban, hogy további útmutatást adna arra vonatkozóan, mit jelent ebben az összefüggésben a megfelelőség. Harmadszor, a reprezentativitás kritériumát tovább pontosítja a 10. cikk (4) bekezdése, amely kimondja, hogy a tanítóadatoknak – a rendeltetéstől függően szükséges mértékben – figyelembe kell venniük és tükrözniük kell azokat a jellemzőket vagy elemeket, amelyek ahhoz a sajátos földrajzi, magatartási vagy funkcionális környezethez kapcsolódnak, amelyben a nagy kockázatú MI-rendszert használni kívánják. Ez a rendelkezés tehát

33 Lásd Frederik Zuiderveen Borgesius: *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making.* Strasbourg, Council of Europe, 2018; #BigData: Discrimination in Data-Supported Decision Making. Bécs, European Union Agency for Fundamental Rights, 2018, 6–8.

34 Ződi i. m. (29. lj.).

arra kényszeríti a fejlesztőket, hogy figyelembe vegyék a rendszer tervezett alkalmazásának konkrét kontextusát. A rendelettervezet a 42. cikk (1) bekezdésében vélelmezi, hogy a kontextus reprezentativitási kritériuma teljesül, ha a tanítóadatok a tervezett földrajzi, viselkedési és funkcionális környezetből származnak.

A rendelettervezet fontos kivételt tesz az általános adatvédelmi rendelet (GDPR) 9. cikk (1) bekezdésében foglalt, az érzékeny adatok feldolgozására vonatkozó tilalom alól. A 10. cikk (5) bekezdése helyesen oldja fel a feszültséget az adatvédelmet és a megkülönböztetésmentességet biztosító jogterületek között. Amennyiben a nagy kockázatú MI-rendszerekkel kapcsolatosan a torzítás nyomon követésének, észlelésének és korrekciójának biztosításához feltétlenül szükséges, az ilyen rendszerek szolgáltatói kezelhetik a személyes adatok különleges kategóriáit, a természetes személyek alapvető jogaira és szabadságaira vonatkozó megfelelő biztosítékokra is figyelemmel, ideértve a legkorszerűbb biztonsági és magánéletvédelmi intézkedések – köztük az álnevesítés, vagy ha az anonimizálás jelentősen befolyásolja a kitűzött célt, a titkosítás – további felhasználására és használatára vonatkozó technikai korlátokat is.[35]

2.2.4. A rendelettervezet szankciórendszere és végrehajtása

A rendelettervezet szigorú szankciót helyez kilátásba (71. cikk), ha az MI-rendszer nem felel meg a 10. cikkben meghatározott követelményeknek, valamint az 5. cikkben szereplő tilalom be nem tartása esetén: legfeljebb 30 millió euró összegű közigazgatási bírságot, vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 6 százalékát kitevő összegű büntetést ír elő; a kettő közül a magasabb összeget kell kiszabni. Amennyiben az MI-rendszer nem felel meg az e rendelet szerinti – az 5. és 10. cikkben meghatározottaktól eltérő – követelményeknek vagy kötelezettségeknek, legfeljebb 20 millió euró összegű közigazgatási bírsággal, vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 százalékát kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni. A rendelettervezet utolsó változatában a 71. cikk (6) bekezdése szerint a szankciók a gazdasági társaság típusától és tevékenységi körétől függően jelentősen, 3, 2 vagy 1 százalékra csökkennek (például kis- és középvállalkozások esetén).

Ezenkívül a rendelettervezetben foglalt, az előzetes tesztelésre, a kockázatkezelésre és az emberi felügyeletre vonatkozó kötelezettségek is elő fogják segíteni egyéb alapvető jogok tiszteletben tartását azáltal, hogy minimálisra csökkentik az MI-n alapuló téves vagy elfogult döntések kockázatát olyan kritikus területeken, mint az oktatás és képzés, a foglalkoztatás, fontos szolgáltatások, a bűnüldözés és az igazságszolgáltatás. Ha továbbra is fennáll az alapvető jogok megsértése, az MI-rendszerek átláthatóságának és nyomon követhetőségének biztosítása, valamint a szigorú utólagos ellenőrzés lehetővé teszi a hatékony jogorvoslatot az érintett személyek számára.

---

35 Philipp Hacker: A Legal Framework for AI Training Data – from First Principles to the Artificial Intelligence Act. 13(2) *Law, Innovation and Technology* (2021) 290–301.; az MI adatvédelmi kérdéseiről bővebben lásd Eszteri Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika Egyetemi Kiadó, 2021, 187–210.

A rendelettervezet uniós szinten létrehozza az Európai Mesterséges Intelligencia Testületet (amely a tagállamok és az Európai Bizottság képviselőiből áll), hogy megkönnyítse az új szabályok összehangolt végrehajtását és biztosítsa a nemzeti felügyeleti hatóságok és a Bizottság közötti együttműködést. Nemzeti szinten a tagállamoknak ki kell jelölniük egy vagy több illetékes hatóságot, köztük egy nemzeti felügyeleti hatóságot, amelynek feladata a rendelet alkalmazásának és végrehajtásának felügyelete volna. A nemzeti piacfelügyeleti hatóságok feladata lenne annak értékelése, hogy a gazdasági szereplők megfelelnek-e a nagy kockázatú MI-vel kapcsolatos rendszerekre vonatkozó kötelezettségeknek és követelményeknek (VIII. cím 3. fejezet). Hozzáféréssel rendelkeznének a bizalmas információkhoz (beleértve az MI-rendszerek forráskódját is), ezért titoktartási kötelezettségek vonatkoznak rájuk. A fokozott átláthatósági kötelezettségek csak az egyének hatékony jogorvoslathoz való jogának gyakorlásához szükséges minimális információkra, valamint a felügyeleti és végrehajtó hatóságok számára szükséges átláthatóságra korlátozódnak, megbízatásuknak megfelelően, ezáltal a szellemi tulajdon védelméhez való jogot [17. cikk (2) bekezdés] sem érintik aránytalanul.

3. Záró gondolatok

A rendelettervezet előremutató, részletesen tartalmazza a nagy kockázatú MI-rendszerekkel szemben támasztott általános (ún. alapvető) követelményeket, míg a részletes műszaki követelményeket elsősorban az európai szabványosítás keretében kidolgozott európai szabványok fogják meghatározni. Bár a részletes műszaki szabványoknak már a III. cím 5. fejezete is nagy szerepet tulajdonít, ezek ma még nagyrészt hiányoznak. Kidolgozásuk döntő fontosságú lesz a javasolt rendelet hatékony végrehajtásához és betartatásához. Ez az észrevétel általánosabban is megfogalmazható a javaslat megfelelőségértékelési mechanizmusának végrehajtásával kapcsolatban. A mesterséges intelligencia rendszerek megfelelőségértékelését olyan műszaki szabályok szerint végzik, amelyeket teljes mértékben a bejelentett szervezetek – azaz a tevékenységükért elvileg díjat kapó magánszervezetek – határoznak meg. Ezért rendkívül fontos annak biztosítása, hogy a nemzeti hatóságok a lehető legnagyobb mértékben felhatalmazást kapjanak arra, hogy demokratikusan ellenőrizhessék, hogyan végzik tevékenységüket ezek a szervezetek és konkrétan hogyan hajtják végre a javaslat szabványait.

A nagy kockázatú MI-rendszerekre vonatkozó kötelező követelmények nagyjából a mesterséges intelligenciával foglalkozó magas szintű szakértői csoport etikai iránymutatásaiban felsorolt „megbízható MI-re vonatkozó követelmények” alapján készültek, és a rendszer forgalomba hozatalát vagy üzembe helyezését megelőzően teljesíteni kell azokat. Ezek különösen az adatminőségre és az adatkezelésre, a dokumentációra és a nyilvántartás vezetésére, az átláthatóságra és a felhasználók tájékoztatására, az emberi felügyeletre, a robusztusságra, a pontosságra és a biztonságra vonatkoznak. Az ilyen kötelező követelmények előírása jelentős előrelépés az MI-rendszerek káros hatásaival szembeni védelem terén. Ugyanakkor a javaslatot továbbra is jelentősen felül kell vizsgálni a nagy kockázatú rendszerek meghatározásának módja és a követelmények tekintetében, amelyek jelenleg egy listán alapulnak, és a rendelkezések előíró jellegűek.

Azzal, hogy a bejelentett szervezetnek jogot biztosít a tanító-, validáló és tesztelési adatokhoz való teljes körű hozzáférésre, valamint a forráskódokhoz való hozzáférés kérelmezésére, a tervezet feszültséget teremt a nagy kockázatú rendszerek fejlesztéséért felelős szervezetek tevékeny-

ségének szabályozására irányuló igény, valamint e szervezetek szellemi tulajdonának védelme között, összhangban a vállalkozás szabadságával és a szellemi tulajdon védelméhez való joggal, amelyeket az Európai Unió Alapjogi Chartája egyaránt véd. Biztosítani kell, hogy a vállalkozások know-how-ja megfelelő védelemben részesüljön, megfelelő titoktartási követelményekkel, és a hozzáférési kérelmeknek célzottnak és a konkrét feladattal arányosnak kell lenniük.

Kritikaként fogalmazható meg, hogy az MI-rendszerek jövőbeli felhasználását nehéz megjósolni, és korai lenne véglegesen rögzíteni a tiltott MI-gyakorlatok listáját. A rendelettervezet szerinti tudatalatti manipuláció tilalma alacsony szintű védelmet nyújt, mivel csak a visszaélések korlátozott körére vonatkozik, és nyitott marad más nem tudatalatti, de manipulatív MI-gyakorlatok előtt.[36]

Irodalomjegyzék

Codagnone, Cristiano – Liva, Giovanni – Rodriguez de las Heras Ballel, Teresa: *Identification and Assessment of Existing and Draft EU Legislation in the Digital Field*. Brüsszel, EU, 2022.

Dobó Judit – Gyaraki Réka: A mesterséges intelligencia egyes felhasználási lehetőségei a rendvédelmi területeken. *Magyar Rendészet,* 2021/4., 67–81. https://doi.org/10.32577/mr.2021.4.3

Dumbrava, Costica: *Artificial Intelligence at EU Borders.* Brüsszel, European Parliamentary Research Service, 2021.

Ebers, Martin et al.: The European Commission's Proposal for an Artificial Intelligence Act: A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). 4(4) *J – Multidisciplinary Scientific Journal* (2021) 589–603. https://doi.org/10.3390/j4040043

Eszteri Dániel: A gépek adatalapú tanításának megfeleltetése a GDPR egyes előírásainak. In Török Bernát – Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika Egyetemi Kiadó, 2021, 187–210.

Franklin, Matija et al.: Missing Mechanisms of Manipulation in the EU AI Act. *The International FLAIRS Conference Proceedings* 35 (2022). https://doi.org/10.32473/flairs.v35i.130723

Georgieva, Ilina – Timan, Tjerk – Hoekstra, Marissa: *Regulatory Divergences in the Draft AI Act. Differences in Public and Private Sector Obligations.* Brüsszel, EU, 2022.

Hacker, Philipp: A Legal Framework for AI Training Data – from First Principles to the Artificial Intelligence Act. 13(2) *Law, Innovation and Technology* (2021) 290–301. https://doi.org/10.1080/17579961.2021.1977219

[36] A rendelettervezet részletes elemzését és a módosítási javaslatokat lásd Nathalie Smuha et al.: How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. *Artificial Intelligence – Law, Policy, & Ethics,* 2021; Martin Ebers et al.: The European Commission's Proposal for an Artificial Intelligence Act: A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). 4(4) *J – Multidisciplinary Scientific Journal* (2021) 589–603.

Hacker, Phillip: Manipulation by Algorithms: Exploring the Traingle of Unfair Commercial Practice, Data Protection and Privacy Law. *European Law Journal,* 2021, 1–34. https://doi.org/10.1111/eulj.12389

Hagendorff, Thilo: The Ethics of AI Ethics: An Evaluation of Guidelines. 30(1) *Minds & Machines* (2020) 99–120. https://doi.org/10.1007/s11023-020-09517-8

Héder, Mihály: A Criticism of AI Ethics Guidelines. *Információs Társadalom,* 2020/4., 57–73. https://doi.org/10.22503/inftars.xx.2020.4.5

Justo-Hanani, Ronit: The Politics of Artificial Intelligence Regulation and Governance Reform in the European Union. 55 *Policy Sciences* (2022) 137–159. https://doi.org/10.1007/s11077-022-09452-8

Karsai Krisztina: A mesterséges intelligencia szabályozásának európai tervezete, avagy algoritmusok térnyerésének előjelei a (büntető) igazságszolgáltatásban. *Forum: Acta Juridica et Politica,* 2021/3., 189–196.

Kecskés Gábor: Az önvezető járművek lehetséges szerepe a fenntartható fejlődési célok elérésében. In Lévayné Fazekas Judit – Kecskés Gábor (szerk.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr, Universitas-Győr Nonprofit Kft., 2020, 155–175.

Madiega, Tambiama – Mildebrath, Hendrik: *Regulating Facial Recognition in the EU.* Brüsszel, EU, 2021.

Mahler, Tobias: Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal. In *Nordic Yearbook of Law and Informatics,* 2021, 245–276. https://doi.org/10.53292/208f5901.38a67238

Mökander, Jakob et al.: The US Algorithmic Accountability Act of 2022 vs. the EU Artificial Intelligence Act: What can They Learn from Each Other? 32(4) *Minds and Machines* (2022) 751–758. https://doi.org/10.1007/s11023-022-09612-y

Roberts, Huw et al.: The Chinese Approach to Artifcial Intelligence: An Analysis of Policy, Ethics, and Regulation. 36(1) *AI & Society* (2021) 59–77. https://doi.org/10.1007/s00146-020-00992-2

Smuha, Nathalie et al.: How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. *Artificial Intelligence – Law, Policy, & Ethics,* 2021. https://doi.org/10.2139/ssrn.3899991

Uuk, Risto: *Manipulation and the AI Act.* Future of Life Institute (2022), https://bit.ly/3qzTqpO.

Vergnolle, Suzanne: Identifying Harm in Manipulative Artificial Intelligence Practices. *Internet Policy Review,* 2021, https://bit.ly/3Clyg1e.

Winfield, Alan F. T. et al.: IEEE P7001: A Proposed Standard on Transparency. 8 *Frontiers in Robotics and AI* (2021). https://doi.org/10.3389/frobt.2021.665729

Zorkóczy Miklós: A mesterséges intelligencia egészségügyi jogi és etikai dimenziói. *MTA Law Working Papers,* 2021/25.

Ződi Zsolt: A mesterséges intelligencia szabályozásának dilemmái. *ITKI blog,* 2020. augusztus 24., https://bit.ly/3jTb5lW.

Ződi Zsolt: Az Európai Bizottság Mesterséges Intelligencia Kódexének tervezete. *Gazdaság és Jog,* 2021/5., 1–3.
Zuiderveen Borgesius, Frederik: *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making.* Strasbourg, Council of Europe, 2018.