CORVINUS LAW PAPERS

ISSN

2416-0415

2/2026

Dudás Gábor

A mesterséges intelligencia jogalanyisága adatvédelmi megközelítésben

Reflexió Metzinger Péter: Mesterséges intelligencia, polgári jogi cselekvőképesség, jogalanyiság című tanulmányára

CORVINUS UNIVERSITY OF BUDAPEST

Corvinus Law Papers

CLP 2/2026

The primary purpose of the Corvinus Law Papers (CLP) is to publish the results of research projects performed by those connected to the Department of Business Law as research reports, working papers, essays and academic papers. The CLP also publishes supplementary texts to be used for practical and theoretical training of students.

Address of the Editorial Board:

Corvinus Law Papers
1093 Budapest, Fővám tér 8. III. emelet 321/A

Publisher:

Corvinus University of Budapest
H-1093 Budapest, Fővám tér 8.

Responsible for the edition:

Dániel Bán

ISSN 2416-0415

A mesterséges intelligencia jogalanyisága adatvédelmi megközelítésben
Reflexió *Metzinger Péter: Mesterséges intelligencia, polgári jogi cselekvőképesség, jogalanyiság*[1] c. tanulmányára

Dudás Gábor
gabor.dudas@uni-corvinus.hu

Absztrakt:

A jogtudományi álláspont mára közel egységesnek mondható abban, hogy nem veti el a mesterséges intelligencia (MI) jogalanyisága elfogadhatóságának lehetőségét, mivel a mesterséges intelligencia polgári jogi szempontból a technikai fejlődéssel dologból egyre inkább személlyé válik. Az MI jogalanyisága szabályozásának szükségessége olyannyira elfogadott, hogy az Európai Unióban közelmúltban elfogadott mesterséges intelligencia rendeletének[2] (AI Act) előkészítése során hosszabb ideig tartotta magát az a koncepció, hogy a rendeletben az elektronikus személyiségi kategória szabályozása is szükséges lenne[3]. Metzinger Péter kiváló tanulmánya szerint polgári jogi szempontból így a kérdés mára szinte már csak az lehet, hogy a technikai fejlődés mikor éri el azt a szintet, amikor már elkerülhetetlen a mesterséges intelligencia jogalanyiságának szabályozása[4].

E körben egyebekben a szakirodalomban az álláspontok megoszlanak a szabályozás szükségességének tényleges realitása és jelenlegi science fiction jellege között. További kérdés, hogy a társasági jogi szabályozáshoz hasonlóan szükséges-e, hogy a mesterséges intelligencia fejlettségétől függően a jogi szabályozás a jogalanyiság különböző szintjeit is szabályozza oly módon, hogy – a társaságokhoz hasonlóan – minél fejlettebb a mesterséges intelligencia, a jogi szabályozás annál erőteljesebben függetlenítse az őt létrehozó vagy működtető személyektől, és annál nagyobb önállósággal ruházza fel jogok és kötelezettségek szerzése, illetőleg felelősségvállalása tekintetében.

Kulcsszavak: mesterséges intelligencia (MI), jogalanyiság, adatvédelem, GDPR

1. Bevezetés

Véleményem szerint a mesterséges intelligencia jogalanyiságának kérdését nem lehet kizárólag jogfilozófiai, illetőleg polgári jogi aspektusok mentén vizsgálni, hanem célszerű, hogy ezt a kérdést más jogterületeket is érintő interdiszciplináris módszerekkel is megközelítsük. Így logikusan adódik, hogy a klasszikus magánjogi oldal mellett a kérdéskört közjogi szempontból

[1] Corvinus Law Papers 3/2025.
[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2024. június 13-i (EU) 2024/1689 RENDELETE
a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról
[3] Ehhez lásd pl. Szentgáli-Tóth Boldizsár: *Robotic personhood and its potential impact to democracy. Should artificial intelligence be citizens and wested with right to vote?*- https://edit.elte.hu/xmlui/bitstream/handle/10831/74964/lotf-771-808%20(1).pdf?sequence=1, letöltés időpontja:2026.0715.
[4] A mesterséges intelligencia (MI) egyre szélesebb körű társadalmi felhasználása jogi reakciókat inspirál. A jelen cikk e lehetséges, netán szükséges jogi reakciókat nem a technológia, hanem a polgári jog klasszikus dogmatikája felől igyekszik megvizsgálni, abból indulva ki, hogy amíg az MI technológiai marad – tehát amíg nem hoz saját, önálló döntéseket –, addig nem állítja a polgári jogot valós kihívások elé, ellenben az már érdemi – polgári jogi és társadalmi – változásokat hozhat, ha az MI polgári jogi értelemében cselekvőképessé válik, mely cselekvőképességnek dogmatikailag szükségszerű vonzata lesz valamiféle jogalanyiság elismerése.

is értékeljük, erre remek példa Szentgáli-Tóth Boldizsár hivatkozott tanulmánya is. A közjogi szempontú értékelés tekintetében pedig szinte kínálja magát az adatvédelmi szempontú vizsgálat, hiszen a mesterséges intelligencia működése elképzelhetetlen adatok gyűjtése, elemzése, és ezekből történő következtetések levonása nélkül, és az MI ezen adatkezelési tevékenysége értelemszerűen nagyszámú személyes adatra is kiterjed. Az adatvédelmi megközelítés szükségessége magából az AI Act-ból is következik, hiszen az AI Act legnagyobb számban az ezzel a jogterülettel való összhang megteremtésére hivatkozik (közel 50-szer), szemben pl. a szintén rendkívül fontos szerzői jogi kérdésekkel (15-ször).
Bármennyire is fontosnak tartja azonban az AI Act a mesterséges intelligencia adatvédelmi követelményeknek megfelelő működését, ha ezt a kérdést részletesebben megvizsgáljuk, akkor – a jelen tanulmányban bemutatottak szerint – látni fogjuk, hogy az általános adatvédelmi rendeletben[5] (általános adatvédelmi rendelet, GDPR) rögzített adatvédelmi követelmények maradéktalan érvényesülése mellett a mesterséges intelligencia csak rendkívül korlátozott módon, vagy egyáltalán nem lehet jogszerűen működtethető. Így „egyiküknek mennie kell", azaz a kívánt összhang megteremtése érdekében vagy a mesterséges intelligencia használatát kell az Európai Unióban a jelenleginél erőteljesebben korlátozni, vagy az uniós adatvédelem elveiből kell engedni. Alapjogi szempontból ugyanakkor nehezen lehet elfogadható a már megszerzett védelmi szint csökkenése a személyes adatok védelme terén, de az Európai Uniónak el kell kerülnie a „gépprombolóvá" válást is, mivel a mesterséges intelligencia használata számtalan gazdasági és innovációs előnnyel kecsegtet. Ezért véleményem szerint elképzelhetetlen a mesterséges intelligencia „betiltása", hiszen a használatából fakadó előnyök miatt ilyenkor nem a használat megszüntetése, hanem az illegális használat a valószínűbb. Így ebben a körben is megfontolandó lehet az a James E. Watson szenátornak tulajdonított mondás, mely szerint „amit nem tudsz megtiltani, annak állj az élére".
Erre is figyelemmel felmerül egy harmadik lehetőség is. Álláspontom szerint ugyanis, ha a mesterséges intelligenciát legalább adatvédelmi szempontból önálló jogalanyisággal ruházzuk fel, azaz – adatvédelmi terminológiával élve – adatkezelési eszközből adatkezelővé emeljük, akkor kialakítható egy olyan jogi modell is, amely változatlan, sőt hatékonyabban érvényesülő adatvédelmi sztenderdek mellett is lehetővé teheti a mesterséges intelligencia működését az Európai Unióban.
Emiatt a jelen tanulmányban amellett kívánok érvelni, hogy a mesterséges intelligencia jogalanyiságának a technikai fejlődéstől függő, legalább részleges elismerése az Európai Unióban nem csupán elvi lehetőségként merül fel, hanem gyakorlati oldalról nézve célszerű is lenne.

2. Az adatvédelmi paradoxon

Az uniós adatvédelmi jog némiképp bizonytalan abban a kérdésben, hogy a személyes adatok védelmét protektív jogként, vagy információs önrendelkezésként azonosítsa[6]. A Német Szövetségi Alkotmánybíróság 1983-as népszámlálási döntése (Volkszählungsurteil) alapján több európai ország (pl. Németország, Hollandia, Magyarország) a személyes adatok védelmét az információs önrendelkezés megvalósulása körébe helyezte, míg az információs önrendelkezés más tagállamokban kevésbé jelentős, ezt a kategóriát egyebekben maga a GDPR

[5] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE
a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
[6] A témához bővebben lásd Dudás Gábor: Az általános adatvédelmi rendelet várható hatása az információs önrendelkezés hazai felfogására In: Bodzási, Balázs (szerk.) A gazdasági jog és az adójog aktuális kérdései 2018-ban : Gazdasági jogi kutatások a Budapesti Corvinus Egyetemen Budapest, Magyarország : Magyar Közlöny Lap- és Könyvkiadó (2018) 223 p. pp. 55-69. , 15 p.

sem használja. Ennek a kérdésnek a témánk szempontjából annyiban van jelentősége, hogy az információs önrendelkezés doktrinája a személyes adatainak védelmét mindenki saját kezébe helyezi, míg a protektív védelem az adatvédelmet uniós, illetőleg tagállami feladatként fogalmazza meg. A két megközelítés közötti különbség így Jóri András találó megfogalmazása alapján az, hogy az információs önrendelkezés esetén a személyes adatok védelme az adatalany (érintett) joga, míg protektív szabályozás esetén ugyanez az adatkezelő kötelezettsége.[7] Mindkét megközelítés mellett kiemelkedő jelentősége van ugyanakkor az érintetti jogoknak, hiszen az információs önrendelkezés oldaláról az egyénnek magának kell megfelelő eszközökkel rendelkeznie önmaga védelmére, protekitív oldalról pedig az uniós és tagállami védelem feladatai hatékonyabban teljesíthetők akkor, ha a védekezésben maguk az érintettek is részt vehetnek.

Az érintetti jogok az általános adatvédelmi rendeletben lépcsőzetesen épülnek fel, minden érintetti jog gyakorlásának az alapja a tájékozottság, és az átláthatóság. Olyannyira fontos alapelv ez, hogy a GDPR az átláthatóság követelményét az alapelvek között elsőként szabályozza[8]. Információs önrendelkezési szempontból a tájékozottság amiatt fontos, mert az érintettek csak akkor tudják megvédeni magukat az adataik jogellenes kezelése esetén, ha információkkal rendelkeznek arról, hogy a személyes adataikat ki, milyen célból, milyen jogalapon, mennyi ideig és hogyan kezeli, kinek és milyen célból adja tovább, illetve milyen módon védi a megsemmisülés és illetéktelen hozzáférés ellen. Az adatvédelem protektív felfogása esetén pedig az átláthatóság amiatt fontos, mert akár a tagállam, akár az unió adott szerve csak akkor tudja kivizsgálni és szankcionálni a jogsértő adatkezeléseket, ha képes tisztázni a tényállást és ennek alapján meg tudja állapítani, hogy mi vezetett a jogsértésre.

Amint azonban arra már a vonatkozó szakirodalom is rámutatott, az MI „fekete doboz” jellege miatt nehéz lehet az MI által hozott döntések magyarázata.[9]

A fejlettebb mesterséges intelligenciák így black boxként működnek, azaz sem a fejlesztő, sem az őket működtető személy nem tudja pontosan, hogy a mesterséges intelligencia milyen úton, milyen adatgyűjtési és adatelemzési tevékenység során jutott el egy adott személyre vonatkozó következtetés meghozataláig.

A mesterséges intelligencia következtetései, döntései ugyanakkor rendkívül jelentősek is lehetnek, például egy hitelkérelem esetén nem szorul különösebb magyarázatra, miért jelent problémát, ha még maga a bank sem tudja, hogy az általa használt MI rendszer részéről milyen okból történt az ügyfél hitelkérelmének elutasítása.

Ilyenkor tehát a klasszikus adatvédelmi felfogás szerinti adatkezelő (fejlesztő, felhasználó – lásd később) nyilvánvalóan nem lehet képes az adatkezelés átláthatóságának biztosítására, hiszen maga sem tudja, mit és miért csinál az MI.

Nyilván fennáll az a lehetőség, hogy ilyen esetben az adatkezelő utólag „megkérdezi” a mesterséges intelligenciát (pl. LIME, SHAP módszerekkel), és a tőle kapott tájékoztatásnak megfelelően tájékoztatja az érintettet.

Ez ugyanakkor nyilvánvalóan nem elégséges megoldás, mert az adatvédelem jelenlegi szintje sok esetben előzetes tájékoztatást követel meg[10]. Az előzetes tájékoztatást pedig a fejlesztő és a felhasználó a fenti esetben értelemszerűen nem képes teljesíteni, ezt csak maga a mesterséges intelligencia lenne képes megtenni, hiszen ő gyűjti az elemzéshez felhasználandó adatokat az érintettektől.

---

[7] Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, PhD-értekezés, 2009. PTE, 323. o.

[8] GDPR 5. cikk (1) bekezdés a) pont

[9] Lizansha Birla-Raj Pipara: Legal identity of artificial intelligence, (43-52) LEGAL IDENTITY OF ARTIFICIAL INTELLIGENCE.pdf, letöltés időpontja: 2026. július 16.

[10] lásd a GDPR 13. cikk rendelkezéseit.

Az adatvédelem protektív felfogása esetén ez a probléma, bár jelentős, de nem életbevágó, hiszen a jogsértések kivizsgálása szintén utólagosan történik az érintett szervek részéről. Természetesen protektív megközelítés esetén sem bagatellizálható ez, hiszen a jogsértés megelőzésére a közhatalmi szervek önmagukban csak kevéssé képesek, az érintettek így itt is jelentős szerepet kell, hogy kapjanak. Ennek oka, hogy a jogsértés veszélyének észlelhetősége az érintettek esetében nagyobb, hiszen ők életszerűen jobban figyelemmel kísérik az adataik sorsát. Információs önrendelkezés oldaláról pedig ez a jogvédelmet teljes mértékben ellehetetlenítené, hiszen az érintettek így elvesztik azt a lehetőséget, hogy a jogsértő adatkezelést megakadályozzák, legfeljebb csak utólag tudják a jogsértést rekonstruálni.
A kérdés ezért a továbbiakban az, hogy mennyiben igaz az az állítás, hogy az MI jogalanyként történő elismerése ezt a problémát megoldhatja. Azaz, máshogy feltéve a kérdést, hogyan lehet képes az MI megadni az adatkezelést érintő szükséges tájékoztatást az érintettek számára.

3. Az átláthatóság biztosítása

Ezzel kapcsolatban előzetesen rögzíteni szükséges, hogy az, hogy az MI képes legyen magyarázni a döntéseit, azaz „magyarázható MI" (explainable AI, XAI) legyen — elvileg nem feltétlenül igényli az MI jogalanyiságának elismerését, hanem ez elsősorban fejlett programozási és algoritmikus megoldások kérdése. Ezen módszerek célja, hogy az MI működését érthetővé tegyék az emberek számára. Például döntési fákat, szabályalapú rendszereket vagy speciális magyarázó algoritmusokat alkalmaznak, amelyek visszavezetik a döntést az input adatokra és a döntési logikára[11].

4. Az MI adatkezelői, adatfeldolgozói minősége

Az uniós adatvédelmi szabályozás két kategóriát különböztet meg az érintettekkel szemben álló, „kötelezetti" oldalon: az adatkezelőket és az adatfeldolgozókat[12]. Az adatkezelők azok a szervezetek, amelyek a személyes adatok kezelését érintő érdemi döntéseket meghozzák, azaz meghatározzák az adatkezelés célját, a kezelendő adatok körét, a megőrzés idejét, az alkalmazandó adatkezelési műveleteket stb. Az adatfeldolgozók pedig azok a szervezetek, akik segítik az adatkezelőt az adatkezelési műveletek elvégzésében, ennek során végrehajtják az adatkezelő adatkezelést érintő utasításait.
Az általános adatvédelmi rendelet alapján az érintetti jogok, így az átláthatóság biztosítása az adatkezelők kötelezettsége.
A klasszikus adatvédelmi megközelítés szerint az MI fejlesztője csak akkor adatkezelő, ha maga használja az MI-t, amennyiben azonban a fejlesztő az MI-t átengedi más felhasználóknak (és az MI kereskedelmi célú felhasználása esetén ez a gyakoribb), akkor adatkezelőnek a felhasználó fog minősülni.
Ugyanakkor viszont kizárólag a fejlesztő lehet képes arra, hogy úgy programozza az MI-t, hogy az MI akár előzetesen, akár utólagosan képes legyen tájékoztatást adni arról, hogy a következtetéseihez milyen adatokat használt fel és miért.
Így abban az esetben, ha ezt a fejlesztő nem végzi el, akkor a felhasználónak két döntési lehetősége keletkezik: vagy nem használja az adott MI-t, vagy vállalja a megfelelő tájékoztatás hiányából fakadó jogsértés kockázatát.
A fejlesztő ugyanakkor ilyen esetben véleményünk szerint nem vonható felelősségre amiatt, mert a megfelelő tájékoztatás megadásához szükséges fejlesztést nem végezte el, hiszen nem ő döntött az MI meghatározott adatkezelési célhoz történő felhasználásáról.

---

[11] Bővebben lásd Pók László: Mesterséges intelligencia és átláthatóság, Mesterséges intelligencia és átláthatóság - GDPR Letöltés időpontja: 2026. július 16.
[12] Lásd GDPR 4. cikk 7-8. pontok

A felhasználó ugyanakkor álláspontunk szerint az adatvédelem objektivizált kárfelelősségi doktrínája[13] alapján akkor is felel az MI jogsértő felhasználásáért, ha egyébként a jogsértés megakadályozására nincsenek eszközei. Az adatvédelem válasza ugyanis erre az, hogy ha valamely adatkezelő nem képes jogszerűen elérni a kívánt adatkezelési célt, akkor ilyen módon ne kezeljen személyes adatokat.
Ez pedig azt eredményezheti, hogy a jog iránt nagyobb mértékben elkötelezett, felhasználónak minősülő adatkezelők az MI-t a jogsértés kockázata miatt nem fogják használni, amivel viszont versenyhátrányba kerülhetnek a jogsértés iránt kevésbé érzékeny felhasználókhoz képest. Ez az irány ugyanakkor nyilvánvalóan nem tekinthető kívánatosnak.
A másik lehetőség persze, hogy a jogi iránt elkötelezettebb felhasználók a versenyhátrány elkerülése érdekében vállalják majd a jogsértés kockázatát. Ez ugyanakkor szintén nem megfelelő irány, hiszen a jogvédelem szintjét nagyban csökkentené.
Mindezek pedig arra a következtetésre vezethetnek, hogy a jogi szabályoznak a fejlesztőket kellene kötelezni, vagy minimálisan inspirálnia XAI-k létrehozására.
A technikai fejlődés függvényében ugyanakkor véleményem szerint ezt az MI jogalanyisággal felruházása segítheti, a következők miatt.
Mivel az adatvédelmi szabályozás közjogi jellegéből adódóan szükségszerűen kogens, ezért valamely jogalany adatkezelői vagy adatfeldolgozói minősége nem választás kérdése, hanem az adott jogalany által végzett adatkezelési tevékenység következménye. Ezért egy „fekete dobozként" működő MI – elvi síkon – szükségképpen csak adatkezelő lehet, hiszen egy adatfeldolgozó nem jogosult a személyes adatok kezelését érintő érdemi döntések meghozatalára, így többek között nem határozhatja meg önállóan a kezelt adatok körét sem. Ezzel szemben egy „fekete doboz" MI működésének lényege éppen az önállóság, a felhasználónak elég csak a feladatot meghatároznia, és az MI maga dönti el, hogy a feladat teljesítéséhez milyen adatokat gyűjt, illetve ezekből milyen következtetésre jut.
Egy MI viszont csak akkor lehet adatkezelő, ha a jogi szabályozás önálló jogalanyisággal ruházza fel. Ez a jogalanyiság a GDPR 4. cikke alapján lényegében bármilyen jellegű lehet, nem szükséges, hogy az MI egyben jogi személyként kerüljön elismerésre. A hatályos uniós szabályozás szerint ugyanis adatkezelő bárki lehet, akár egy képviselő vagy egy önállóan működő szervezeti egység is.
A fent kifejtettek alapján természetesen nem minden MI esetében merül fel az önálló jogalanyiság megszerzésének szükségessége, csak azoknál, amelyek black boxként működnek, és részt vesznek személyes adatokat érintő döntési folyamatokban
Az adatkezelői minőségből ugyanakkor a korábban jelzettek szerint objektivizált felelősségvállalási kötelezettség is keletkezik, egy adatkezelés jogszerűségéért elsődlegesen az adatkezelő kell, hogy a felelősséget viselje, hiszen az adatkezelést érintő döntéseket is ő hozta meg.
A MI felelőssége megteremtésének lehetősége így a jogalanyiság és ezzel együtt az adatkezelői minőség elfogadásának egyik legfontosabb, ha nem a legfontosabb kérdése. Egyebekben végül éppen ez a problematika volt az, ami miatt az EU Bizottság az AI Act előkészítése során elvetette az MI elektronikus személyiségének szabályozását. A legfontosabb ellenérv az elektronikus személyiséggel szemben ugyanis az volt, hogy az MI önálló felelőssége mentesítheti a fejlesztőket és a felhasználókat a saját felelősségvállalási kötelezettségük alól, így ez végső soron az MI felelőtlen használatához vezethet.
Álláspontom szerint ugyanakkor a Bizottság ezen kifogása annyiban nem tekinthető kardinálisnak, mivel az MI adatkezelői felelősségének elismerése valójában nagy valószínűséggel nem járhat azzal, hogy a fejlesztők és a felhasználók mentesüljenek a felelősségük alól.

[13] Lásd a GDPR 82. cikkét

Ennek oka pedig szintén abban a szabályozási logikában rejlik, amely az adatkezelőt adatkezelővé minősíti, azaz az érdemi döntéshozatali képesség és lehetőség kérdésében.
A hatályos uniós szabályozás szerint ugyanis nemcsak egy szervezet minősülhet adatkezelőnek valamely adatkezelés tekintetében, hanem amennyiben a személyes adatok kezelésének célját, eszközeit többen közösen határozzák meg, akkor ezen szervezetek közös adatkezelőnek minősülnek, akik egyetemleges felelősséggel tartozhatnak egymás tevékenységéért is.
Ennek alapján álláspontom szerint az MI nem lehet önálló adatkezelő. Ennek oka, hogy bár az adatkezelés módját egy „fekete dobozként" működő MI maga határozza meg, de az adatkezelés célját mindig a felhasználó adja meg, egy MI soha nem kezd saját döntése alapján kutatni egy témában, a feladatot és a tevékenység irányát a felhasználó határozza meg. Emellett szintén a felhasználó az, aki dönt arról, hogy a feladatra MI-t vesz igénybe.
A felhasználó és az MI közös adatkezelői minősége pedig arra vezet, hogy az esetlegesen jogsérelmet szenvedett érintettek az egyetemleges felelősség miatt a felhasználótól kártérítéshez juthatnak az MI jogsértése esetén is, az egyéb szankciók viszont már az MI-t közvetlenül is sújthatják, áttételesen bevonva ezáltal a felelősségi láncba a fejlesztőket is.
Így tehát az MI jogalanyiságának és ezáltal adatkezelői minőségének elismerése adatvédelmi szempontból ugyan nem elengedhetetlen feltétele az AI Act és a GDPR összehangolásának, de nagymértékben elősegítheti ezt, hiszen megoldást jelenthet arra a paradoxonra, mely szerint az adatkezelőnek minősülő felhasználók az érintetti jogok biztosítására önmagukban nem képesek, az erre képes fejlesztők viszont adatkezelői minőség hiányában az érintetti jogok biztosítására nem kötelesek.