Ványik Paszkál Adrián

joghallgató (PTE ÁJK), az ÓNSZ Bűnügyi Tagozatának tagozatvezetője

A GDPR és AI Act viszonya a mesterséges intelligencia korában

I. Bevezetés

Az adatvédelem, mint jogintézmény viszonylag fiatal, mégis a digitális technológiák gyors fejlődése miatt napjainkra az uniós jog egyik legdinamikusabban változó területévé vált. Bár az Európai Parlament és a Tanács (EU) 2016/679 rendeletével 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 (továbbiakban: GDPR)[1] 2016-os elfogadásával az Európai Unió átfogó és egységes keretet teremtett a személyes adatok kezelésére, a mesterséges intelligencia (továbbiakban: MI) megjelenése újraértelmezte az adatvédelem határait. Az MI rendszerek tömeges adatfelhasználása, automatizált döntéshozatala és a *„black box"* jelenség mind olyan kihívások, amelyek a GDPR egyes rendelkezéseinek gyakorlati alkalmazhatóságát is kérdésessé tehetik.[2] Ennek a helyzetnek az uniós válasza a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló rendeletet (továbbiakban: AI Act)[3], amely elsőként próbálja jogszabályi szinten keretbe foglalni a MI technológiai és alapjogi kockázatait.

A személyes adatok kezelése a digitális környezetben ma már állami, vállalati és a magánszféra szereplőinek mindennapi tevékenységének része.[4] A *Big Data*-korszakban a gyorsan keletkező és sokféle adat tömeges feldolgozása vált az MI működésének alapjává. A gépi tanulási modellek – különösen a mélytanulás – bonyolult adatműveletekkel, nagyléptékű

[1] 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) (továbbiakban: GDPR)

[2] *Üveges* István: A feketedoboz jelensége és következményei a mesterséges intelligencia alapú technológiákban. Wolters Kluwer. https://jogaszvilag.hu/a-jovo-jogasza/a-feketedoboz-jelensege-es-kovetkezmenyei-a-mesterseges-intelligencia-alapu-technologiakban/ (2025. 12. 01.)

[3] Az Európai Parlament és Tanács (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 (a mesterséges intelligenciáról szóló rendelet) (továbbiakban: AI Act)

[4] *Rákos* Dóra: A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében. Opuscula Iuvenum Excellentissima (ELTE ÁJK) 2019/2. sz. 1. o.

mintázatfelismeréssel és önálló döntési mechanizmusokkal operálnak.[5] Ez a folyamat azonban gyakran vezet átláthatatlan döntéshozatalhoz, ami szükségessé tette a magyarázható MI (explainable AI, XAI) megjelenését.[6] Az adatok minősége, jogszerű felhasználása és reprezentativitása így a rendszer megbízhatóságának és az alapjogok érvényesítésének kulcselemévé vált.[7]

A kutatásom célja annak vizsgálata, hogy a GDPR – mint általános adatvédelmi rendelet – és az AI Act – mint speciális, technológiafókuszú szabályozás – miként viszonyul egymáshoz. A két rendelet hasonló, de eltérő logikát követ, ugyanakkor közös céljuk a személyek védelme és a magánszféra tiszteletben tartása a MI korában. A kutatásomban ennek megfelelően külön-külön bemutatom a GDPR és az AI Act főbb rendelkezéseit, majd elemzem azok összeilleszthetőségét, az esetleges normatív feszültségeket. Végül arra is kitérek, hogy a két rendelet kapcsolatából milyen következtetések vonhatók le, és milyen javaslatokkal lehetne segíteni a jelenlegi szabályozási helyzet pontosítását.

II. Adatkezelés

II.1. Az adatkezelés alapelvei

A rendelet külön fejezetben határozza meg azokat az elveket, amelyek minden adatkezelés során érvényesülnie kell, így ezek az alapelvek határozzák meg az adatkezelés általános keretrendszerét. Ezen elvekből első olvasatra is egyértelműen kitűnik, hogy elsődleges az érintettek védelme. Ezek alapján az adatkezelés során alapvető fontosságú a jogszerűség, a tisztességes eljárás és az átláthatóság biztosítása („jogszerűség, tisztességes eljárás és átláthatóság" elve). Minden adatgyűjtésnek előre meghatározott, egyértelmű és jogszerű célokkal kell rendelkeznie, és az adatokat nem szabad ezen célokkal össze nem egyeztethető módon kezelni. Kivételt képeznek ez alól azok az esetek, amikor az adatokat közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai célból kezelik („célhoz kötöttség"). Az adatkezelés céljainak szempontjából az adatoknak megfelelőnek és relevánsnak kell lenniük, és csak a szükséges mértékben szabad őket gyűjteni („adattakarékosság"). Az adatok pontosságát és naprakészségét folyamatosan biztosítani kell, így minden pontatlan adatot azonnal törölni vagy helyesbíteni kell („pontosság"). Az adatok tárolása csak addig tarthat, ameddig az a kezelés céljainak eléréséhez szükséges, kivéve, ha az adatok

[5] European Parliamentary Research Service (EPRS): How artificial intelligence works. European Parliament. https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-how-artificial-intelligence-works.pdf (2025.12.01.)
[6] Maria *Frasca* et. al.: Explainable and interpretable artificial intelligence in medicine: a systematic bibliometric review. Discover Artifical intelligence 2024/4. sz. 15. 3-4. o.
[7] European Union: Open data and AI: A symbiotic relationship for progress. European Union. https://data.europa.eu/en/publications/datastories/open-data-and-ai-symbiotic-relationship-progress (2025.12.01.)

közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai célból kerülnek további kezelésre. Ilyen esetekben is fontos, hogy megfelelő technikai és szervezési intézkedések biztosítsák az adatok védelmét és az érintettek jogainak megőrzését („korlátozott tárolhatóság"). Az adatkezelés biztonságának biztosítása érdekében megfelelő technikai vagy szervezési intézkedéseket kell alkalmazni, amelyek védelmet nyújtanak az adatok jogosulatlan vagy jogellenes kezelése, valamint a véletlen elvesztés, megsemmisítés vagy károsodás ellen („integritás és bizalmas jelleg"). Végül, az adatkezelő felelős a fent említett szabályok betartásáért, és képesnek kell lennie a megfelelés igazolására, így biztosítva az elszámoltathatóságot az adatkezelés teljes folyamata során („elszámoltathatóság").[8]

Ahogy korábban már említettem, fő cél az érintettek védelme az adatkezelés során, amit az azzal éri el a rendelet, hogy az adatkezeléssel kapcsolatban szigorú követelményeket támaszt az adatkezelővel szemben amellett, hogy őket terheli elszámoltathatóság elvével is, amely nem csak azt jelenti, hogy az adatkezelő felelős az előírások betartásáért, de szükség esetén ő köteles igazolni a jogszerű eljárást. A gyakorlatban ez egy hatalmas terhet jelent az adatkezelő számára, mert ez magába kell foglalnia az érintettek megfelelő informálását az eljárással és jogaikkal kapcsolatban, saját szervezeti és működési szabályzatok kialakítását és pontos dokumentációt a teljes tevékenységeivel kapcsolatban egy esetlegesen felmerülő hiba elhárítása érdekében.

II.2. Az érintett jogai

A rendelet következő elengedhetetlen része az érintettek jogai, amely az alapelvekhez hasonlóan saját fejezetben került meghatározásra. A személyes adatok védelmének középpontjában az információs önrendelkezési jog áll. Emiatt, ahogy az alapelvekből is látszott, a rendelet egyik célja egy olyan rendszer kialakítása, amely képessé teszi az érintetteket, hogy rendelkezhessenek a személyes adataikról és adatkezelésről.

Az érintettek jogait három fő csoportba lehet sorolni az alapján, hogy a jog mely alapelv érvényesülését szolgálja.[9] Az első ilyen csoport, amely az átláthatóságot biztosítja és ide tartozik, hogy az érintetteknek joguk van tájékoztatáshoz már az adatkezelés kezdete előtt is, amelynek magába kell foglalnia az adatkezelés célját és körülményeit. Ez a tájékoztatás az adatkezelő kötelessége, amelynek az érintett kérelme nélkül is eleget kell tennie. További átláthatósághoz kapcsolódó jog a tájékoztatáshoz sokban hasonlító hozzáféréshez való jog. A legnagyobb különbség a kettő között, hogy ennek az esetében nemcsak az adatkezelés előtt, hanem annak folyamata során tud informálódni az adatkezeléssel kapcsolatban. Fontos más eleme ennek, hogy

[8] GDPR II. Fejezet
[9] *Péterfalvi* Attila – *Révész* Balázs – *Buzás* Péter: Magyarázat a GDPR-ról. Wolters Kluwer Hungary, Budapest 2018. (szerk.) 140-210. o.

az érintett jogosult az adatait megkapni, illetve felszólítani az adatkezelőt, hogy az közvetlen formában más adatkezelőnek továbbítsa az adatait. Ebből kifolyólag a másik nagy különbség, hogy ezzel csak az érintett kérelmére lehet élni.[10]

A második csoport, amely a pontosság elvét juttatja érvényre. Ide tartozik a helyesbítéshez való jog, ami alapján az érintett személy kérheti, hogy az adatkezelő indokolatlan késedelem nélkül javítsa ki a pontatlan személyes adatait. Az adatkezelés céljának figyelembevételével az érintett jogosult arra is, hogy kérje hiányos személyes adatainak kiegészítését is. Ilyen még a törléshez való jog, aminek, noha az adattakarékosság elve szerint az adatkezelési cél elérése után kéne megtörténnie, de a rendelet lehetőséget ad az érintettnek arra, hogy már a cél megvalósulása előtt is kérhesse személyes adatainak törlését. Fontos itt megemlíteni, hogy a törlési jog gyakorlása, nevével ellentétben, nem mindig eredményezi a személyes adatok tényleges törlését vagy fizikai megsemmisítését. Az adatvédelmi jogban a törlés azt jelenti, hogy a személyes adatokat olyan módon kell felismerhetetlenné tenni, hogy az érintett és az adatok közötti kapcsolat ne legyen helyreállítható, így például az anonimizálás esetében.[11] A harmadik pedig az adatkezelés korlátozásához való jog, amelynek megfelelően a rendeletben meghatározott esetekben az érintett kérheti, hogy az adatkezelő korlátozza az adatkezelést.[12]

Harmadik csoportba sorolhatjuk azokat a jogokat, amelyek nem konkrét alapelvek érvényesülését szolgálják. Ide tartozik a tiltakozáshoz való jog, illetve az automatizált döntéshozatal esetén érvényesülő jog. A tiltakozáshoz való jog már részben a második csoportban tisztázásra került, hiszen az érintett tiltakozásának egyik lehetséges következménye a személyes adatok törlése, illetve az adatkezelés korlátozása. A különbség abban rejlik, hogy tiltakozási joggal egyedül a jogos érdeken alapuló, illetve a közérdekű célból végzett adatkezelések esetén lehet élni és ebben az esetben a tiltakozás jogosságának eldöntésénél az ellentétes oldalon álló jogos okok közötti elsőbbség lesz a meghatározó. Végül pedig az utolsó jog, amelyet említ a rendelet az automatizált döntéshozatal esetén, amely alapján az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené. Ez a már többször említett technológiai változásokra adott válasz, amely próbálja megakadályozni, hogy az érintettek pusztán az adataik felhasználásával váljanak különböző döntések alanyaivá.

[10] GDPR 2. szakasz
[11] Vö. 7. jegyzet
[12] GDPR 3. szakasz

III. A két rendelet viszonya

III.1. Az alapelvek teljesülése

A GDPR és az AI Act viszonyának vizsgálatának kezdetén fontos kitérni az alapelvek közötti különbségekre, mivel ezek alkotják a keretrendszert. A GDPR, amely az adatvédelem középpontjában áll, az adatkezelés átláthatóságára és *compliance* jellegére helyezi a hangsúlyt. Ezzel szemben az AI Act célja a MI-val működő rendszerek kockázatainak kezelése, különös tekintettel a magas kockázatú rendszerekre, amelyek szigorúbb követelményeket igényelnek. Így fontos, hogy az AI Act hogyan utal vissza, egészíti ki vagy esetlegesen módosítja a GDPR által meghatározott elveket a MI rendszerek sajátosságainak kezelésére.

A MI rendszerek személyesadat-kezelését továbbra is a GDPR alapelvei határozzák meg, mivel az AI Act nem hoz létre önálló adatkezelési jogalapot és nem írja felül a hatályos adatvédelmi szabályokat. A jogszerűség és tisztességes eljárás követelményei így változatlanul fennállnak, bár az AI Act nem nevesíti kifejezetten a *„fairness"* fogalmát az előírásai – különösen a magas kockázatú rendszerekre vonatkozó adatminőségi, dokumentációs és emberi felügyeleti követelmények – közvetetten e célok megvalósítását szolgálják. Az átláthatóság ugyanakkor kifejezetten központi elem, amely a felhasználó tájékoztatásától az üzemeltetési logika alapvető bemutatásáig terjed. A célhoz kötöttség elve az AI Act rendszerében a magas kockázatú MI-rendszerek precíz célmeghatározási és dokumentációs kötelezettségei révén érvényesül, míg az adattakarékosság – bár önállóan nem jelenik meg – a szükségesség és arányosság alapelvein, valamint a „privacy by design" megközelítésen keresztül épül be a szabályozásba. Az AI Act a pontosság elvét tovább szigorítja, hiszen a magas kockázatú MI-rendszerek esetében a megfelelő minőségű, reprezentatív és torzításmentes adatkészleteket a jogszerű és megbízható működés előfeltételeként határozza meg, hangsúlyozva a követelmény adatvédelmi és alapjogi jelentőségét. A tárolási korlátozás elve tekintetében az AI Act nem tartalmaz új szabályokat, ami különösen a hosszú távú tanulásra és nagyméretű adattömegekre épülő rendszereknél vet fel gyakorlati kérdéseket. E körben az anonimizálás jelenti azt az eszközt, amely lehetővé teszi a személyes adatoktól elszakított tovább feldolgozást. Az integritás és bizalmasság védelmét mindkét rendelet a kockázatalapú technikai és szervezeti intézkedések előírásával biztosítja. A GDPR általános biztonsági követelményeit az AI Act a magas kockázatú rendszerek esetén speciális előírásokkal – folyamatos kockázatmonitorozással, adat- és modelldokumentációval, az emberi felügyelet megerősítésével és a megfelelő szakértelem biztosításával – egészíti ki. Ezzel a szabályozás a technológiai transzparencia növelését és az alapjogi sérelmek megelőzését célozza.

III.2 A kockázatalapú megközelítések párhuzamai

A kockázatalapú megközelítés mind a GDPR, mind az AI Act szabályozási logikájának meghatározó eleme. A két rendelet különböző aspektusból, de közös célkitűzéssel igyekszik biztosítani, hogy az egyének alapvető jogai és szabadságai ne sérüljenek az adatvezérelt és automatizált döntéshozatali rendszerek működtetése során. A GDPR alapján előírt adatvédelmi hatásvizsgálat (*Data Protection Impact Assessment*, továbbiakban: DPIA)[13] és az AI Act által bevezetett alapjogvédelmi hatásvizsgálat (*Fundamental Rights Impact Assessment*, továbbiakban: FRIA)[14] egyaránt megelőző jellegű, ex ante eszköz, amely az adatkezelési vagy MI-technológiai műveletek bevezetése előtt feltárja és értékeli a potenciális jogsérelmek kockázatát.

A DPIA a GDPR értelmében minden olyan adatkezelési tevékenység esetén kötelező, amely az érintettek jogait és szabadságait súlyosan veszélyeztetheti – különösen új technológiák, például MI alkalmazása esetén.[15] Az EDPB iránymutatása alapján a DPIA három tipikus esete közé tartozik: (1) automatizált döntéshozatal joghatással, (2) különleges adatok vagy bűnügyi adatok nagy volumenű kezelése, valamint (3) nagyléptékű, nyilvános megfigyelés.[16] Ezekhez számos további kategória társulhat, amelyeket a nemzeti adatvédelmi hatóságok külön határozhatnak meg. Az IEEE 2022-es kutatása szerint egyes tagállamok – például Ausztria, Dánia, Németország, Görögország és Csehország – minden MI-alapú adatkezelés esetén kötelezővé teszik a DPIA-t.[17] Az AI Act ezzel szemben a magas kockázatú MI-kat a III. mellékletben foglalt osztályozási keret alapján azonosítja, olyan szempontok szerint, mint:

(1) felhasználási szektor,
(2) alkalmazási cél,
(3) használt technológia típusa,
(4) üzemeltető, valamint
(5) érintetti kör.[18]

E szempontok alapján az AI Act meghatározza azokat az eseteket, ahol FRIA elvégzése kötelező. Noha az AI Act a FRIA-t önálló kötelezettségként határozza meg a magas kockázatú rendszerek kapcsán, lényegi kapcsolat áll fenn a DPIA-val, mivel a rendszerek gyakran személyes adatok

[13] GDPR 35. cikk
[14] AI Act 27. cikk
[15] Vö. 11. jegyzet
[16] EDPB/WP29: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"
[17] Tytti *Rintamäki* et. al.: High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications. OSF Preprints, 2023. 1-20. o. https://tyttikatariina.github.io/High-Risk-Categorisations-in-GDPR-vs-AI-Act/ (2025.12.01.)
[18] Delaram *Golpayegani* – Harshvardhan J. *Pandit* – Dave *Lewis*: To Be High -Risk , or Not To Be - Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards. In 2023 ACM Conference on Fairness, Accountability, and Transparency. Chicago, 2023. 905–915. o.

feldolgozásán alapulnak. Az IEEE kutatása a két mechanizmus összehasonlító elemzése során kimutatta, hogy az AI Act III. mellékletében szereplő 25 magas kockázatú alkalmazási kategóriából 23 esetben a GDPR szerinti DPIA is kötelező – ami jelentős szabályozási átfedést jelez. Ez a szoros integráció igazolja, hogy a GDPR alkalmazása nem szorul vissza az AI Act hatálybalépésével, hanem épp ellenkezőleg: az új szabályozás gyakran feltételezi a GDPR követelményeinek teljesülését.

A gyakorlati kérdések szempontjából kulcskérdés, hogy a DPIA és a FRIA hogyan viszonyulnak egymáshoz tartalmi és eljárási szempontból. Az AI Act lehetővé teszi, hogy egy korábban elvégzett DPIA kiegészítésként szolgáljon a FRIA számára, amennyiben az tartalmilag lefedi az alapjogi kockázatok lényegi elemeit. Ez a megközelítés hivatott lehetőséget adni a hatásvizsgálatok integrált elvégzésére, és elősegíteni a költséghatékony, átlátható és következetes megfelelési gyakorlat kialakítását, különösen transznacionális kontextusban. Mindazonáltal a tagállamok közötti eltérő jogértelmezési gyakorlat – például a DPIA kötelezettség nemzeti szintű bővítése – nehezítheti az egységes végrehajtást. A jövőbeli jogharmonizációban ezért kulcsszerep juthat az AI Act végrehajtási rendeleteinek és a kapcsolódó soft law eszközöknek (pl. útmutatók, gyakorlati példák), amelyek segíthetnek a két vizsgálattípus alkalmazási kereteinek pontosításában.

III.3. Átláthatóság az MI-rendszerekben

Az európai adatvédelmi szabályozás egyik alapkövetelménye az átláthatóság, amely alapelvként végigvonul a teljes jogi keretrendszeren. Célja, hogy az adatkezelési folyamatok átláthatók maradjanak, biztosítva az elérhető és értelmezhető információhoz való hozzáféréssel az érdekvédelmi eszközök gyakorlását.[19] De a gyakorlat szempontjából nem elhanyagolható, hogy mit értünk pontosan átláthatóság alatt különösen olyan esetekben, amelyekben több jogszabályt kell párhuzamosan alkalmazni és azok részben eltérnek. Ennek a kérdésnek az eldöntésében segít nekünk a GDPR 39. preambulumbekezdése.[20] Ebben az esetben az európai jogalkotó a központba a tájékoztatást, illetve a kommunikációt helyezi az átláthatóság körvonalazásakor, hogy ezen keresztül a teljes adatkezelés átláthatósága biztosított legyen. Mégis a GDPR 12. cikke részben eltér és úgy követeli meg az átlátható tájékoztatást, hogy átláthatóság fogalmán kívül határozza meg az érthetőség, a könnyű hozzáférhetőség, a világos és közérthető nyelvezet követelményeit.[21] Így ezek értelmezése érdekében az Európai Adatvédelmi Testület iránymutatásait célszerű megvizsgálni. A

[19] *Hohmann* Balázs – *Fábián* Adrián – *Szőke* Gergely László: The Shades of the Concept of Transparency on the Horizon of European Technology Law and Platform Regulation. Juridical Tribune – Review of Comparative and International Law 15./1. sz. 44–62. o.
[20] GDPR 39. preambulumbekezdés
[21] GDPR 12. Cikk

több kiadott iránymutatás között, amely az átláthatóság témájával foglalkozik kiemelt jelentőséggel bír a 2018-ban kiadott.[22] Ez alapján az átláthatóság megköveteli, hogy az adatkezelők világos és érthető, jogi zsargontól mentes információkat adjanak az érintetteknek, amelyek pontosak, naprakészek és könnyen hozzáférhetők. Ezeket a feltételeket új technológiák esetén is biztosítani kell annak ellenére, hogy új nehézségeket teremtenek az átláthatóság gyakorlati megvalósíthatósága ellen. Emiatt az EDPD egyik 2021-ben kiadott iránymutatása értelmében az adatkezelőknek különös figyelmet kell fordítaniuk az algoritmusok és az automatizált döntéshozatali rendszerek átláthatóságára, mivel ezek a technológiák gyakran bonyolultak és nehezen érthetőek az érintettek számára, nem véletlenül nevezik őket gyakran „fekete dobozoknak".[23] Emiatt mostanra már elsődleges fontosságú, hogy az AI Act hogyan képes a GDPR sokszor bizonytalan értelmezésű átláthatósági követelményeinek megfelelni és azokat az MI-k sajátoságaira tovább vezetni.

Az MI rendszerek gyakran bonyolult adatkezelési folyamatokat foglalnak magukban, amelyek a „black box" hatás miatt nehezen átláthatóak még a technológia fejlesztője vagy üzemeltetője számára is.[24] Ha ezek a rendszerek személyes adatokat is kezelnek, akkor a jogi megfelelőség biztosítása érdekében egyszerre szükséges megfelelni a fent ismertetett átláthatósági követelményeknek, valamint az algoritmikus döntéshozatalra vonatkozó egyéb szabályozásoknak. Ezért az AI Act 47. preambulumbekezdése előírja, hogy a magas kockázatú MI-rendszerek esetében megfelelő dokumentációval és egyértelmű tájékoztatással kell ellátni a felhasználókat, hogy megértsék és helyesen alkalmazzák a rendszereket.[25] Ezzel szemben a rendelet nem határoz meg fogalmat az átláthatóságra s csupán annyit ír elő, hogy működésüket úgy kell alakítani, hogy kellően átláthatóak legyenek ahhoz, hogy a felhasználók értelmezhessék a rendszer kimenetét és megfelelően használhassák azt, nagy kockázatú MI-rendszerek esetén.[26] Ez alapján a GDPR fent említettek szerint nem teljesen egyértelmű körülírása az irányadó. Ezzel együtt az AI Act az átláthatóság körülírása helyett az értelmezhetőség és tájékoztatás minimumkövetelményeit határozza meg.[27] A minimumkövetelmények megfogalmazása során részben az adatvédelmi jogban már meglévő elemeket integrál, amelyek a felhasználók számára egyértelmű, hozzáférhető, és tömör információk biztosítását célozzák. Ezen túlmenően viszont új követelményeket is felállít, amelyek a technológiai sajátosságokra és a felmerülő problémákra vonatkoznak. Ezek a követelmények előírnak egy olyan dokumentum (használati utasítás) létrehozását, amely az átláthatóság és

[22] EDPB: Guidelines on Transparency under Regulation 2016/679
[23] Vö. 3. jegyzet
[24] Frank *Pasquale*: The Black Box Society: The Secret Algorithms Behind Money and Information. Harvard University Press, Cambridge 2016. 59-100. o.
[25] AI Act Preambulum (47) bekezdés
[26] AI Act 13. cikk (1) bekezdés
[27] AI Act 13. cikk (2)-(2) bekezdés

tájékoztatás követelményeinek kíván megfelelni. Ebben a dokumentumban olyan információknak kell szerepelni, amelyek elősegítik a jogérvényesítést – meghatalmazott képviselő adatai – illetve a rendszer működésével kapcsolatosak – célja, pontossága, kockázatok –. Fontos azonban megemlíteni, hogy a használati utasítás kötelező tartalmi elemei révén a rendelet további előírásai is hozzájárulhatnak az átláthatóság fokozásához.[28] A jogszabály szövegében kifejezetten nincs megemlítve, hogy ezek hogyan kapcsolódnak az átláthatósághoz. Ezen kívül a tudományos diskurzusban is fellelhetők eltérő vélemények ezzel a témával kapcsolatban.[29]

III.4. Érintetti jogok biztosítása MI környezetben

A kutatásom utolsó kérdése az érintetti jogok érvényesülését vizsgálja. Bár a GDPR részletes és erős érintetti jogosultságokat biztosít, ezek gyakorlása a MI-k összetett, sokszor önállóan adaptálódó adatkezelési mechanizmusai miatt gyakran nehézkessé válhat.

A helyesbítés joga korlátozottan alkalmazható olyan MI-rendszerekben, ahol a személyes adatok folyamatosan újra felhasználják és aggregálják. Az AI Act nem dolgoz ki olyan speciális technikai vagy eljárási megoldásokat, amelyek a korrekciós jog érdemi érvényesítését biztosítanák ilyen környezetben. A tiltakozáshoz való jog esetében hasonló hiányosságok mutatkoznak. Noha az AI Act jelentős dokumentációs és bizonyos mértékű átláthatósági kötelezettségeket ír elő, ezek nem teremtik meg annak feltételeit, hogy az érintett ténylegesen megakadályozhassa adatainak MI-alapú felhasználását. A rendelet nem tartalmaz olyan eljárási garanciákat vagy hatásmechanizmusokat, amelyek közvetlenül biztosítanák a tiltakozás gyakorlati érvényesülését. A tájékoztatáshoz való jog szintén csak részben teljesül. Az AI Act által előírt információszolgáltatás jellemzően általános, rendszer-szintű, és nem terjed ki az érintett egyedi adatainak kezelésére vonatkozó részletes információkra. Ez a hiány jelentősen korlátozza az információs jogok tényleges gyakorlását, mivel a megfelelő tájékoztatás hiányában az érintett nem tudja felmérni, hogyan és milyen célból használják fel adatait.

Összességében az AI Act – bár a dokumentációs követelmények és a használati utasítás révén hozzájárul az átláthatósághoz – csak korlátozottan képes támogatni a GDPR által kialakított érintett-központú jogvédelmi rendszert. A rendelet elsősorban rendszer-szintű megfelelőségi követelményeket fogalmaz meg, amelyek nem minden esetben fordíthatók le közvetlenül érvényesíthető érintetti jogosultságokra.

---

[28] Ida *Varošanec*: On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI. In: International Review of Law, Computers & Technology. Taylor & Francis, London 36(2) 2022. 95–117. o.

[29] Madalina *Busuioc* - Deirdre *Curtin* - Marco *Almada*: Reclaiming transparency: contesting the logics of secrecy within the AI Act. European Law Open 2.1, Cambridge 2023, 79-105. o.

IV. Konklúzió

Az AI Act jelentős előrelépést jelent a MI kodifikációjában, és céljai alapvetően összhangban állnak a GDPR által kialakított keretrendszerrel. A rendelet kockázatalapú megközelítése különösen fontos, mivel ez a logika már a GDPR-ban is központi szerepet tölt be, és elősegíti, hogy az AI-rendszerekre vonatkozó előírások illeszkedjenek a meglévő adatvédelmi struktúrákhoz. A rugalmas és általános, kockázati szinteken alapuló szabályozás egyfelől támogatja a jogi megfelelést, másfelől teret enged az innovációnak is, hiszen a szolgáltatók így saját működésükhöz igazíthatják a megfelelési intézkedéseket. A rendelet által előírt kötelezettségek hozzájárulhatnak a technológiába vetett bizalom erősítéséhez.[30] Ugyanakkor véleményem szerint több ponton látható, hogy az AI Act csak részben felel meg a GDPR által támasztott elvárásoknak. Különösen az átláthatóság fogalma körül jelentkeznek értelmezési bizonytalanságok: a szabályozásból nem mindig egyértelmű, hogy az átláthatóság az információk hozzáférhetőségére, érthetőségére vagy a működés magyarázhatóságára vonatkozik-e. Kérdés az is, hogy a „használati utasítás", mint az átláthatóság gyakorlati eszköze valóban képes-e betölteni ezt a funkciót, különösen akkor, ha összetett technikai információkat kell laikus felhasználók számára közérthető módon közvetíteni. Az AI Act végrehajtásának részletei és az ex ante elemzések gyakorlati hatékonysága szintén további pontosítást igényel. E hiányosságok ellenére a rendelet több olyan iránymutatást is ad – például az MI-jártasság fejlesztésének ösztönzésével[31], a gyakorlati kódexek támogatásával[32] vagy az MI Hivatal létrehozásával[33] –, amelyek hosszú távon erősíthetik a szabályozási környezet koherenciáját. Ha ezek a mechanizmusok megfelelően integrálódnak az EDPB iránymutatásaival és a bevált gyakorlatokkal, reális esély nyílik a jelenlegi eltérések csökkentésére.

Az alábbiakban három konkrét javaslatot mutatok be, amelyek elősegíthetik a jelenlegi szabályozási hiányosságok csökkentését. Elsőként elengedhetetlen egy részletes uniós iránymutatás az átláthatóság egységes értelmezésére. Ahogy korábban kifejtettem, az átláthatóság alapvetően befolyásolja az MI-rendszerek fejlesztését, működését és társadalmi elfogadottságát; a fogalom tisztázása ezért mind a szolgáltatók, mind a felhasználók számára kulcsfontosságú. Másodszor, úgy látom, hogy szükség lenne olyan jogérvényesítési megoldások pontosítására vagy kiegészítésére, amelyek kifejezetten a MI-rendszerek működéséből adódó problémákra reagálnak. Az AI Act önmagában nem hoz létre külön eljárásokat, ami önmagában nem hiba, hiszen ezek a GDPR

[30] *Hohmann* Balázs – *Kollár* Gergő: Reflections on the data protection compliance of AI systems under the EU AI Act. Cogent Social Sciences 11/1. sz. 20 o.
[31] AI Act 4. cikk
[32] AI Act V. fejezet 4. szakasz 56. cikk
[33] AI Act VII. fejezet 1. szakasz 64. cikk

hatáskörébe tartoznak. A gond inkább ott kezdődik, hogy a MI-rendszerek összetettsége miatt a meglévő jogok gyakorlása sokszor nehezebbé válik. Emiatt indokoltnak tűnik olyan kiegészítő mechanizmusok kialakítása, amelyek valóban segítik az érintetteket abban, hogy egy hibás vagy jogsértő rendszerrel szemben hatékonyan és érdemben felléphessenek. Harmadszor, a DPIA és a FRIA közötti kapcsolat, valamint a két vizsgálattípus eredményeinek újrahasznosíthatóságának tisztázása, jelentősen csökkentené a szolgáltatók adminisztratív terheit. Mivel mindkét vizsgálat a jogsérelem-megelőzésre épül, a kötelezettségek harmonizálása a megfelelés egyszerűsítését és a gyakorlati alkalmazás egységesítését is elősegítené.