



**37. Országos Tudományos Diákköri Konferencia
Állam- és Jogtudományi Szekció**

Budapest, 2025. március 24–26.

Rendező intézmény:
*Károli Gáspár Református Egyetem
Állam- és Jogtudományi Kar*



Állam- és Jog-
tudományi Szekció

**Adatvédelem az új digitális korszakban: A
GDPR és a mesterségesintelligencia rendelet
összefüggései és kihívásai**

**Kézirat lezárásának dátuma:
2024.12.09.**

A dolgozat szerzőjeként kijelentem, hogy csak angol nyelvről magyarra történő fordításhoz használtam mesterséges intelligenciát. Ez ChatGPT és DeepL használatával történt.

Tartalomjegyzék

ADATVÉDELEM AZ ÚJ DIGITÁLIS KORSZAKBAN: A GDPR ÉS A MESTERSÉGESINTELLIGENCIA RENDELET ÖSSZEFÜGGÉSEI ÉS KIHÍVÁSAI	1
I. BEVEZETÉS	4
I.1. AZ ADATVÉDELEM JÖVŐJE A MESTERSÉGES INTELLIGENCIA KORÁBAN	4
I.2. A MESTERSÉGES INTELLIGENCIA	5
I.3. ADATOK ÉS ALAPIJOGOK	8
I.4. MI RENDELET HÁTTERE	9
I.5. AZ AI ACT MEGALKOTÁSÁNAK MOZGATÓRUGÓI	11
I.6. AZ AI ACT CÉLKITŰZÉSEI	13
I.7. ÖSSZSHANG	14
II. GDPR SZEREPE ÉS HATÁSA AZ ADATVÉDELEMRE: ELŐZMÉNYEK, ALAPELVEK, JOGOK ÉS KÖTELEZETTSÉGEK.....	14
II.1. ALAPFOGALMAK.....	14
II.2. ADATKEZELÉS ALAPELVEI	16
II.3. AZ ÉRINTETT JOGAI.....	17
II.4. KÖTELEZETTSÉGEK, AVAGY A MIKRO-, KIS- ÉS KÖZÉPVÁLLALKOZÁSOK KIHÍVÁSAI	19
II.5. JOGORVOSLAT, FELELŐSSÉG ÉS SZANKCIÓK	20
II.6. GDPR ALKALMAZÁSA MESTERSÉGES INTELLIGENCIA ESETÉBEN	21
III. A MESTERSÉGES INTELLIGENCIA RENDELET.....	23
III.1. A MESTERSÉGES INTELLIGENCIA RENDELET BEVEZETÉSE	23
III.2. FOGALOMMEGHATÁROZÁSOK	24
III.3. MI RENDSZEREK OSZTÁLYOZÁSA	26
III.4. KIBERBIZTONSÁG ÉS AZ ADATVÉDELEM	27
III.5. AI ACT ÖSSZEFOGLALÁS.....	28
IV. KÖVETKEZTETÉSEK A KÉT RENDELET VISZONYÁVAL ÖSSZEFÜGGÉSBEN	29
IV.1. ALAPELVEK TELJESÜLÉSE	29
IV.1.1. JOGSZERŰSÉG, TISZTESSÉGES ELJÁRÁS ÉS ÁTLÁTHATÓSÁG.....	29
IV.1.2. Célhoz kötöttség és adattakarékosság	29
IV.1.3. Pontosság	30
IV.1.4. Korlátozott tárolhatóság.....	30
IV.1.5. Integritás és bizalmas jelleg	30
IV.2 A KOCKÁZATALAPÚ MEGKÖZELÍTÉSEK PÁRHUZAMAI	31
IV.3. ADATVÉDELMI HATÁSVIZSGÁLAT ÉS AZ ALAPVETŐJOGI HATÁSVIZSGÁLAT VISZONYA	32
IV.3. ÁTLÁTHATÓSÁG AZ MI-RENDSZEREKBEN	35
IV.4. ÉRINTETTI JOGOK BIZTOSÍTÁSA MI KÖRNYEZETBEN.....	37
V. KONKLÚZIÓ	38

I. Bevezetés

I.1. Az adatvédelem jövője a mesterséges intelligencia korában

Amikor a személyes adatokról és azok védelmét biztosító intézményesített rendszerről beszélünk egy relatív fiatal jogintézményre gondolunk. Mégis az adatvédelem kérdése az elmúlt évtizedekben egyre nagyobb figyelmet kapott hiszen a digitális világ fejlődésével folyamatosan új kihívások jelennek meg a személyes adatok biztonsága terén. Az Európai Unió szemével úgy tűnhetett, hogy ennek a kérdése 2016-ban hosszú időre megoldódott 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), de a mesterséges intelligencia (továbbiakban: MI) megjelenésével ez a megváltozott és újra megkérdőjelezhető, hogy hogyan tudjuk az új kihívásokkal szemben megvédeni személyes adatainkat. George Orwell 1984 című világhírű regényének szállóigévé vált „A NAGY TESTVÉR SZEMMEL TART!” mondata napjainkban kis csavarral talán aktuálisabb, mint valaha. A kis testvér, vagyis a vállalatok, akiknek a fogyasztók egyre növekvő mértékben vannak kiszolgáltatva a MI segítségével eddig sosem látott módszerekkel tudnak a tömegekkel és az azt alkotó magánszemélyekkel szemben visszaéléseket elköveti. Az elmúlt évek robbanásszerű technológiai fejlődésének, az internet, illetve az okostelefonok széleskörű elterjedésének következtében a mindennapi életünk során egyre többször kerülünk olyan helyzetbe, amikor valamilyen személyes információt gyűjtenek, tárolnak és kezelnek rólunk, a viselkedésünkről vagy a személyes preferenciánkról. Ilyen adatok megtalálhatóak különböző vállalatoknál, állami szerveknél és bizonyos esetekben magánszemélyeknél is egyaránt ezért ezek megfelelő szabályozása egy rendkívül bonyolult és nehézkes feladat a jogalkotónak.¹ Ennek a problémának a megoldását Magyarország esetében megkönnyíti, hogy az Európai Unió elfogadta 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 szóló rendeletet (továbbiakban: AI Act).

Így kutatásomban a személyes adatok védelmét és az MI összefüggéseit vizsgálom a GDPR, mint általános adatvédelmi rendelet és az új AI Act, mint a korábbihoz képest speciális

¹ Rákos Dóra: *A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében. Opuscula Iuvenum Excellentissima* 2019. (1), 1. o.

szabályon keresztül. Az új rendelet hatályba lépése új szabályozási környezetet teremt, amely jelentős hatással van az adatvédelem területére is. A megváltozó jogi keretrendszer számos olyan rendelkezést tartalmaz, amelyek új kihívásokat és feladatokat jelentenek a jogalkalmazók, a címzettek, és a kutatók számára is. A kutatás célja ezen új AI Act és a már meglévő adatvédelmi szabályozások kritikai összehasonlítása, valamint annak vizsgálata, hogy ezek miként befolyásolják a MI alkalmazását. Továbbá annak azonosítása, hogy mely rendelkezések ütközhetnek egymással, és milyen következtetések vonhatók le az adatvédelmi szabályozás fejlődésének irányairól a MI kontextusában. A kutatásban ezért először bemutatom külön-külön a GDPR-t és az AI Act-t majd ezek után a kettő közötti viszonyra térek ki először elméleti szinten majd gyakorlati példák bemutatásával és végül az esetlegesen felmerülő hibákra ajánlok megoldásokat

I.2. A mesterséges intelligencia

A dolgozat témájából adódóan az adatvédelem az új AI Act és a GDPR tükrében ezért fontos először magát a mesterséges intelligenciát, mint technológiát és működését röviden bemutatni. Ez megkönnyíti, hogy a jogi szabályozások különösen az AI Act alkalmazhatóságát és hatásait a megfelelő technológia alapok ismeretében tárgyalhassam, így a tanulmányomban jobban rávilágíthatok a szabályozás és a technológia, illetve az elmélet és a gyakorlat összefüggéseire és ellentétére.

Az utóbbi pár évben, ha azt mondjuk, hogy MI akkor a legtöbb embernek a ChatGPT vagy más Large Language Modell (nagy nyelvi modell) illetve a képszerkesztő rendszerek jutnak eszébe, de ezzel ellentétben a mesterséges intelligenciával akármilyen feladatot el lehet végezni bizonyos határokon belül. Az MI számítástechnikai rendszerek összetett hálózatán alapszik, amelyek különböző feladatokat végeznek az emberi gondolkodáshoz és intelligenciához hasonlóan. Az ilyen rendszerek célja, hogy képessé tegyék a gépeket, hogy önállóan döntést hozzanak, tanuljanak és problémákat oldjanak meg, akárcsak az emberek. Ezt a nagy rendszer az által éri el, hogy különböző algoritmusokat használ, amelyek bemeneti adatok alapján képesek valamilyen eredményt előállítani. Emiatt a MI első lépése az adatok gyűjtése. Ez lehet valós idejű például érzékelők vagy kamerák, illetve előre felvett adatok, mint a különféle adatbázisok. Ezek után jön az adatok előkészítése, hogy a nyers formában meglévő adatokat az algoritmusok számára alkalmazható formára alakítsák. Ide tartozik az adattisztítás, amelynek során a nyers adatokat megszabadítják a hibáktól, hiányzó vagy irreleváns részekről, majd az adatnormalizálás következik, vagyis, hogy az adatokat azonos alapokra hozzák, mint például 1-esekre és 0-ákra változtatása majd végül az így kapott adatokat olyan formára

alakítják, amely már alkalmas a rendszer tanítására. A következő nagyobb rész a modellezés, aminek a keretében kiválasztják, hogy a gépi tanulás, illetve mélytanulási modellek közül melyik az előnyösebb a rendszer tanítására. A gépi tanulás (Machine learning) keretében a számítógépek megtanulnak feladatokat megoldani, anélkül, hogy minden lépést előre meghatároznánk nekik, mint egy hagyományos alogaritmus esetében. Ebben az esetben az adatok alapján tanulnak és azok alapján döntenek, illetve készítenek előrejelzéseket. Például egy egyszerű eset egy olyan rendszer, amelynek az a feladata, hogy felismerje a mókusokat a képen a rendszer ezt azáltal tanulja meg hogy megmutatunk neki több száz vagy akár ezer képet, amin van vagy nincs mókus és a gép megtanulja azokat a jellemzőket – mint a mókus formája vagy színe – amelyek alapján felismerheti a mókust és a később bevitt képeken megpróbálja megtippelni, hogy van e rajta mókus vagy sem. A mélytanulás pedig a gépi tanulás egy sokkal fejlettebb speciális formája, aminek az esetében úgynevezett neurális hálózattokat használnak a rendszerek, amelyek hasonlóan az emberi agyhoz rétegeken keresztül dolgozzák fel az adatokat és ezek a rétegek segítik a számítógépet abban, hogy összetettebb feladatokat is megoldjon. Ebben az esetben a rétegek különböző jellemzőket tanulnak meg például a képfelismerés esetében az egyik réteg megtanulja felismerni a formákat egy másik a színeket és egy bonyolultabb réteg pedig felismeri, hogy mi van a képen végül egy végső kimeneti réteg pedig döntést hoz hogy van e a képen mókus vagy sem. Például, ha egy számítógépnek azt akarjuk megtanítani, hogy megmondja melyik képen van mókus és melyik van madár akkor mélytanulás esetében a gép egyre pontosabban megtanulja a formákat, színeket és más jellemzőket és ez alapján dönt. A legnagyobb különbség, hogy míg a gépi tanulás egyszerűbb, könnyebben szabályozható algoritmusokat használ, a mélytanulás több adatot és számítástechnikai kapacitást igényel, de bonyolultabb feladatok elvégzésére képes. A modellezés után jön az értékelés, aminek a keretében különböző szempontok alapján értékelik a kapott eredményeket és ha nem kielégítőek akkor finom hangolják a modellt vagy egyéb adatokat gyűjtenek a modell javítására. Ezek után pedig bevezetik a modellt, vagyis alkalmazni kezdik a valós világban.² Ez jelentős lépés mivel nagy különbség szokott lenni a rendszer létrehozása és valós alkalmazása során bevitt adatok között.

Ezekből látszik, hogy milyen szoros kapcsolat van a MI alapú rendszerek és az adatok között. A rendszerek alapvetően adatokra épülnek különösen a tanulási fázisban amikor pusztán a nagy mennyiségű adat bevitelével tanul a rendszer. Ahogy az előbb említettem az adatok több

² European Parliament: *How artificial intelligence works*. European Parliament. <https://www.sipotra.it/wp-content/uploads/2019/03/How-artificial-intelligence-works.pdf> (2024. 10. 30.)

forrásból származhatnak akár direkt akár véletlenszerűen, ezért fontos az adatok egyező alapokon történő kezelése, ami nehézkes tud lenni főleg azok nagy mennyisége miatt, de a rendszer tanulása szempontjából előnyösebb, ha az adatkészlet minél nagyobb és változatosabb hiszen így tudunk a legjobban megbizonyosodni arról, hogy a rendszer a legtöbb gyakorlatban felmerülő problémával találkozni tudjon a biztonságos tanulási fázis során. Emellett fontos az adatok minősége is, hiszen az alacsony minőségű zajos, pontatlan vagy akár torzított adatok ugyancsak hibás eredményekhez vezethetnek. A gyakorlatban különböző módszereket alkalmaznak a használt adatok minőségének javítására például az adatvalidáció vagyis, hogy a bemeneti adatoknak bizonyos követelményeknek kell megfelelni. Így egyértelműen látszik, hogy a MI alapú rendszerek hatékonysága nem csak a használt algoritmusoktól függ, hanem az adatok minőségétől és pontos előkészítésétől is. Ahogy azt korábban említettem ez jelentős problémákhoz vezethet, mert ha a rendszer tanítása során alkalmazott adatok túlságosan mesterségesek akkor az a valós alkalmazáskor hibákhoz vezethet. A rendszer ugyanis könnyebben hoz döntéseket olyan adatok alapján, amelyek kifejezetten azért hoztak létre, hogy azok alapján döntést tudjon hozni. Ez megtévesztő lehet hiszen hamis képzetet tud kialakítani és azt mutatni, hogy a rendszer képes megfelelően ellátni a célját. Azonban a valóságban leggyakrabban az adatokat nem szakértők – például adatvédelmi vagy informatikai szakértők – dolgozzák fel, vagy maguk az adatok hiányosak, ami a rendszer működését jelentősen korlátozza. Sok példa van, amelyeknek egy részét a későbbiekben majd részletesen elemzem is, amikor a rendszer a gyakorlatban használhatatlanná válik vagy pedig csak aránytalanul nagy nehézségekkel tudja ellátni a célját.³

Miután tisztáztam a MI technológia legalapvetőbb elveit szót kell ejteni a legfontosabb fogalmakról. Az első ilyen a Big Data, ami a nagy mennyiségű, gyorsan változó, különféle típusú adatok kezelésére utal, amely olyan nagy és összetett, hogy a hagyományos adatfeldolgozó módszerekkel már nem lehetséges elég hatékonyan kezelni. Az adatokról írtaknak megfelelően általában a három V-vel szokták jellemezni, amik a Volume (az adatok mennyisége), Velocity (sebesség az adtok keletkezésének és feldolgozásának sebessége), Variety (az adatok változatosága) utal. Az utóbbi időben viszont a technológia változások folytán ezek az alap jellemzők kibővültek további V-vel, mint például a Verocity (a hitelesség

³ *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> (2024.10.30.)

az adatok pontossága és megbízhatósága) és a Value (az adatokból kinyerhető értéke) utal.⁴ A Big Data a 21. század egyik legnagyobb változásaiban játszik szerepet és valószínűleg a jövőben is fontos kérdések kapcsolódnak majd hozzá, mint hogy az ebből fakadó előnyökkel, illetve veszéllyel, hogy lehet megbirkózni. Már most komoly kérdésként merül fel, hogy az állami intézmények hogyan képesek megküzdeni ezzel a jelenséggel, miközben a magánszféra aktívan kiaknázza ennek a lehetőségeit.⁵ Hasonlóan fontos fogalom a Blackbox effektus (fekete doboz hatás), ami a MI azon problémájára utal, hogy azok belső működése, döntéshozatali folyamata és logikája nem átlátható vagy pedig nem érthető akár a szakemberek számára sem. Ez azt jelenti, hogy nem egyértelmű, hogy a rendszer a bemeneti adatok alapján hogyan jutott az adott döntésre és ez rejtve marad, mint a fekete dobozon tárolt adatok. Ez a probléma főleg a mélytanulási modell esetében merül fel hiszen a neurális hálózatok olyan bonyolult több rétegből álló rendszert alkot, amely emberi elmével nehezen értelmezhető és mivel ezek a rendszerek önállóan tanulnak fejlesztenek ki szabályokat. Ez kivételesen jelentős dilemma tud lenni például az egészségügyben, ahol kockázatok mérlegelése során szerepet játszik a döntéshozatali folyamat.⁶ Erre a hibára válaszként megjelent a magyarázható MI kutatási terület (explainable AI, XAI) aminek a célja, hogy a MI döntéshozatali folyamatait áttekinthetőbbé és világosabbá tudják tenni.⁷

I.3. Adatok és alapjogok

Az Európai Unió eleinte csupán gazdasági integrációként indult, de az elmúlt évtizedekben egyre több figyelmet fordít az alapvető jogokra és alapértékekre. Ezt legjobban az Európai Unió bíróságának gyakorlatából lehet levezetni, ami kezdetben elutasító jelleget mutatott, de a Stauder-ügytől kezdve megjelent az alapjogvédelem uniós szinten is. Ez egyre nagyobb teret nyert azóta különböző módokon, mint például az alapjogok egyik sarokkövének

⁴ Szűts Zoltán és Yoo Jinil: *Big Data, az információs társadalom új paradigmája*. Információs Társadalom 16(1), 2016. 8-28. o.

⁵ Forgács Imre: *A Big Data, avagy kezdjük el gondolkodni a közigazgatás új feladatairól*. In: Fazekas Marianna (szerk.): *Gazdaság és közigazgatás: tanulmányok Ficzer Lajos tiszteletére*. Budapest, ELTE Eötvös Kiadó, 2015. 123-133. o.

⁶ Üveges István: *A feketedoboz jelensége és következményei a mesterséges intelligencia alapú technológiákban*. Wolters Kluwer. <https://jogaszvilag.hu/a-jovo-jogasza/a-feketedoboz-jelensege-es-kovetkezményei-a-mesterseges-intelligencia-alapu-technologiakban/> (2024.10.30.)

⁷ Maria Frasca et. al.: *Explainable and interpretable artificial intelligence in medicine: a systematic bibliometric review*. 2024. 4(15) 1. o.

az Alapjogi Chartának az elfogadása, a Lisszaboni szerződéssel 2007-ben lezárt reformok vagy akár az Emberi Jogok Európai Egyezményéhez való csatlakozás. De több jogi kötő erővel nem rendelkező célkitűzés és más politikai állásfoglalás is erre utal. Ezek a változások valóban számtalan előnnyel járnak, de komoly kihívásokat is hozhatnak magukkal, különösen az adatok kezelésével kapcsolatban. Hiszen az új technológiák, például a MI csak jelentős mennyiségű és változatos adattal képes megfelelően működni. Ezzel szemben az alapvető jogok és a GDPR által létrehozott magas szintű adatvédelmi követelmények ezt nagy mértékben meggátolják.

Találhatunk olyan EU-n kívüli példákat, ahol megengedőbb adatvédelmi szabályozás van hatályban, mint az Egyesült Államok, ahol emiatt például a Google és Facebook számára nyíltabban van lehetőség az adatok gyűjtésére. Így tudott a Google az egyik vezető fejlesztő vállalattá válni a MI területén, mert az adatok szabad áramlása jó hatással van a fejlesztésére. De ezzel együtt meg kell említeni, hogy a magánélet védelme kevésbé hangsúlyossá válik így és az egyesült államokban az ilyen megengedőbb szabályozás miatt gyakoriak az adatvédelemmel kapcsolatos adatbiztonsági incidensek. A jogalkotónak ilyen éles ellentétekkel kell megbirkóznia, hogy hatékonyan tudja a MI területét kodifikálni.⁸

I.4. MI rendelet háttere

Az Európai Unió 1994-es Bangemann jelentés óta foglalkozik a digitális politikával. De először a 2014 és 2019 közötti Jean-Claude Juncker korszak hozott nagy lendületet, majd a 2019-ben megtartott Európai Parlamenti választás és Bizottság elnökváltása. A Parlament prioritását a választások után a biztonság, átláthatóság és a megkülönböztetéstől mentesség jellemzi, amelyek a személyek jogainak biztonságban tartásának szempontjából meghatározóak. Ursula von der Leyen a 2019-es júliusi beszédében kiemelt jelentőséget biztosított a digitális korra méltó Európa koncepciójának, amelynek a keretében kötelezettséget vállalt arra, hogy a bizottság mandátumának megkezdését követő 100 napban előterjesztést fog tenni a MI emberi és etikai következményeivel kapcsolatos jogalkotásra.⁹ Ez az „ambiciózus unió”, amely keretében 2020-ban új 10 éves szakpolitikai programot adtak ki, amelyben elsődleges a digitalizáció, illetve 2020. februárjában egy négy dokumentumból álló új stratégiai

⁸ Richard Lawne: *GDPR vs U.S. state privacy laws: How do they measure up?*. Fieldfisher. <https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure> (2024.10.30.)

⁹ The von der Leyen Commission's priorities for 2019-2024
https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf
(2024.10.30.)

csomagot tett közé a bizottság az „Európai adatstratégia”, a „Jelentés a mesterséges intelligencia, a dolgok internete és a robotika biztonsági és felelősségi vonatkozásairól”, és az „Európa digitális jövőjének megtervezése” és a téma szempontjából legfontosabb a „Fehér Könyv a mesterséges intelligenciáról” című dokumentum.¹⁰ A másik mesterséges intelligenciáról szóló dokumentum felhívja a figyelmet az adatfüggőség veszélyeire, vagyis a korábbiakban leírtaknak megfelelően az adatok pontossága és relevanciájának szükségességére. A Fehér Könyv a 2018-as vállalásoknak tesz eleget. Ez a bizottság általános iránymutatása a MI területén, amely ismételten kiemeli az adatgazdaság és a technológia közötti kapcsolatot. Ezeknek a dokumentumoknak kötelező ereje jogilag nincsen és a fő céljuk az, hogy a kommunikációt megindítsák és a jogalkotást orientálják. A Fehér könyv rövid idő alatt az érdekelt felek közreműködésével széles körű konzultációt indított és jelentős támogatást kapott, de több komoly kritika is érte. A legfőbb problémaként a hibás, illetve hiányzó fogalommeghatározásokat emelte ki. Ilyen fogalom volt, például a MI, amiről több eltérő definíció is készült, amiatt mert a bizottság és egy magas szintű szakértői csoport különböző módon közelítették meg a MI-t.

A Fehér könyv célját végül sikeresen elérték és a bizottság benyújtotta a javaslatot, ami egy rendes jogalkotási eljárás megkezdését eredményezte.¹¹ A tervezet kapcsán felmerült egy fontos kérdés, mégpedig a kockázat és a személyes adat fogalmainak meghatározása. Ezek a definíciók alapvetőek a szabályozás értelmezése és alkalmazása szempontjából, azonban a rendelet szövegéből hiányoztak, ami bizonytalanságokat eredményezett.

A kockázat fogalma különösen fontos a MI alkalmazásainál, mivel az MI rendszerek bevezetése és működtetése számos kockázattal járhat, beleértve az adatvédelmi, etikai és biztonsági kockázatok is. A pontos meghatározás hiányában nehéz egyértelműen dönteni, hogy milyen kockázatokra vonatkoznak a szabályozás előírásai, és hogy ezeket hogyan kell kezelni. A személyes adat fogalmának tisztázása szintén elengedhetetlen, mivel a MI rendszerek rendszerint dolgoznak fel ilyen adatokat, és a GDPR már egy jól megalapozott és bevett

¹⁰ Európai Bizottság: *Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése*. European Union. <https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52020DC0065> (2024.10.30.)

¹¹ Jonas Schuett: *Risk Management in the Artificial Intelligence Act*. European Journal of Risk Regulation. 2024. 15(2) 367-385. o. <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> (2024.10.30.)

definíciót biztosít erre a fogalomra. Ez a helyzet felveti azt a kérdést, hogy szükséges-e új, a mesterséges intelligenciára szabott definíciók bevezetése, vagy pedig a GDPR által használt korábbi fogalmak alkalmazása elegendő-e. Ha új definíciók kidolgozására van szükség, ezeknek figyelembe kell venniük a MI sajátosságait és a technológia fejlődéséből adódó új kihívásokat, amellett, hogy a GDPR által már meghatározott általános előírásoknak is meg kell felelnie. Ugyanakkor, ha a GDPR-ban meglévő fogalmak használhatóak, akkor ezek alkalmazása biztosíthatja a jogi koherenciát és az egyértelműség megőrzését a szabályozási környezetben. A bizottság és a parlament közötti megállapodás nehézkes és hosszadalmas volt, aminek a főbb okai az alkalmazott modellből eredő kockázat alapú csoportosítással kapcsolatos eltérések a különböző alkalmazott MI-val működő programok között, az ipari szektor tiltakozása, mivel a megelőző számítások alapján túlságosan nagy mértékű gazdasági terhet jelentett volna. Emellett kardinális kérdés volt a biometrikus adatokkal kapcsolatban felmerült kételyek, hiszen ebben a körben erősebben megjelent az államok érdeke, mivel számos területen alkalmazásban így például a bűnüldözés és határrendészet esetében. Emellett ezek az adatok szigorú védelem alá esnek miután különösen érzékeny adatnak minősülnek a GDPR alapján.

Fontos kiemelni az Európai Unió egyik jelentős hatását, amelyet gyakran Brüsszel-hatásnak neveznek. A "Brüsszel-hatás" arra utal, hogy az Unió szabályozási normái globális szabvánnyá válnak, még akkor is, ha eredetileg csak az Unión belül voltak kötelező érvényűek. Ez a jelenség azért következik be, mert az Unió gyakran szigorú szabályokat vezet be különböző területeken, mint például az adatvédelem, a környezetvédelem és a fogyasztóvédelem, amelyeket a globális vállalatoknak is be kell tartaniuk, ha az Unió piacán is kívánnak működni. Emellett az Unió szabályozásai gyakran példaértékűek más országok számára is, amelyek átveszik ezeket a szabályokat és beépítik a saját jogrendszerükbe. Így amikor az emberiség elérte azt a technológia szintet amikor már képessé vált az MI „életre keltésére” nem meglepő, hogy az Európai Unió kíván ezeknek a kutatásoknak, tanulmányoknak és szabályozásoknak az élére törni és meghatározni azt a szabványt, amely a továbbiakban fokmértéknek számít majd más országok számára és így megvalósítani a Brüsszel-hatást ezen a jövőt teljesen átszövő területen is.

I.5. Az AI Act megalkotásának mozgatórugói

A MI olyan gyorsan fejlődő technikák, amely széles körű gazdasági és társadalmi előnyökhöz vezethet az iparágak és a társadalmi tevékenységek teljes spektrumában.¹² Ahogy

¹² AI Act indoklás 1.1.

az idő előrehaladtával az emberek egyre több és több egymástól eltérő munkafolyamatokat próbálnak meg emberi tevékenységtől függetleníteni így egyre invazívabb informatikai rendszerekre van szükség. Mára már mindennapi kérdés, hogy a lakossági felhasználásra szánt okostelefonok és más gépek monitorozzák az emberi viselkedést és reakciókat annak érdekében, hogy a legtökéletesebben tudják az igényeket kielégíteni, így magától értetődő, hogy a modern gépek esetében a kiindulópont a személyre szabottság. Emellett azonban egyre magasabb igény jelentkezik olyan rendszerek kialakítására, amely képes az emberek jövőbeni akár esetlegesen felmerülő igényeinek kielégítésére. Az ilyen feladatok elvégzésére szinte csak MI alapú öntanuló rendszerek alkalmazásával van lehetőség. Ezek a rendszerek optimális esetben a szükséges adatokat úgy szerzik meg rólunk, hogy mi engedélyezzük, hogy a különböző személyes adatainkhoz hozzáférhessenek, de az elmúlt években több botrány alapja volt már, hogy engedély nélkül elérték ezeket az információkat és akár vissza is élhettek velük. Ilyen esetekben a személyiségi jogaink nem csak oly módon sérülnek, hogy a privát adataink jogosulatlanul mások birtokába kerülnek, de ilyen módon akár jelentős tömegek gondolkodásának és viselkedésének befolyásolására is lehetőség nyílik anélkül, hogy az áldozatok ebből bármit is észlelhetnének. Ebből látszik, hogy ugyanazok az elemek és technikák, amelyek elősegítik a MI társadalmi-gazdasági előnyeit, új kockázatokkal vagy negatív következményekkel is járhatnak az egyének vagy a társadalom számára.¹³ A technológia változás és a folyamatos kihívások mellett így nem meglepő, hogy az EU egyfajta kiegyensúlyozott megközelítés mellett döntött a MI szabályozásának esetében, hogy egyszerre tudja biztosítani az nemzetközi versenyben betöltött szerepét, illetve az európaiak számára uniós értékeknek, az alapvető jogoknak és az alapelveknek megfelelően kifejlesztett és működő új technológiák előnyeit. ¹⁴Emellett azt sem szabad figyelmen kívül hagyni, hogy ez nem lenne az első alkalom, amikor a jogalkotók csak mérsékelt lépéseket tesznek egy sürgető kérdés megoldása érdekében, és végül alulmaradnak a megoldás keresésében. A gyors technológiai fejlődés miatt a jog csak ideiglenes védelmet tud nyújtani azoknak, akik úttörő szerepet vállalnak. Éppen ezért lehet, hogy egy másik, talán modernebb megközelítésre lenne szükség a probléma megoldásához.

¹³ Vö. 3. jegyzet

¹⁴ Jean-Marc Leclerc: *IBM Statement on the Landmark EU AI Act*. IBM. <https://newsroom.ibm.com/IBM-Statement-on-the-Landmark-EU-AI-Act> (2024.10.30.)

I.6. Az AI Act célkitűzései

A rendelet megalkotásának indokai mellett a Tanács 2017-es októberi ülésének¹⁵, 2019-es következtetésének¹⁶, 2020-as következtetésének¹⁷, illetve az Európai Parlament 2020 októberi állásfoglalásai figyelembevételével a Bizottság 4 fő célkitűzéssel nyújtotta be a javaslatot. Így:

1. annak biztosítása, hogy az Unióban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek és tiszteletben tartsák az alapvető jogokat és alapértékeket,
2. a jogbiztonság biztosítása és az ilyen rendszereket érintő innovációba történő befektetések elősegítése,
3. az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása,
4. MI-rendszerek tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése.¹⁸

A célkitűzések elérésének érdekében a rendelet minimumkövetelményeket határoz meg, hogy elkerülje a technológiai fejlődés indokolatlan korlátozását vagy akadályozását, illetve az ezzel járó költségek növelését, így megpróbálva elérni egy időtálló rugalmasságot, amelyet a kockázatalapú megközelítéssel egészít ki. Az Európai Unióban (EU) a túlszabályozás elkerülése rendkívül fontos, mivel a túlzott szabályozás negatív hatással lehet az innovációra, a versenyképességre és a gazdasági növekedésre. A területen az egyik legfontosabb példa a túlszabályozás veszélyeire a digitális szolgáltatások és a technológiai szektor szabályozása. Az EU-ban a GDPR bevezetése számos pozitív hatással járt, de egyes kritikusok szerint a túlzottan szigorú adatvédelmi követelmények különösen a kis- és középvállalkozásokat terhelik meg.¹⁹ Emellett a rendelet érvényesítését a már meglévő rendszere épülő tagállami szintű irányítási

¹⁵ Európai Tanács, [Az Európai Tanács ülése \(2017. október 19.\) – Következtetés](#), EUCO 14/17, 2017, 8. o.

¹⁶ Az Európai Unió Tanácsa, [Mesterséges intelligencia b\) Következtetések a mesterséges intelligenciáról szóló összehangolt tervről – A következtetések elfogadása](#) 6177/19, 2019.

¹⁷ Az Európai Unió Tanácsa, [Az elnökség következtetései – Az Alapjogi Chartáról a mesterséges intelligencia és a digitális átalakulás összefüggésében](#), 11481/20, 2020.

¹⁸ Vö. 12. jegyzet

¹⁹ Aryamala Prasad: *Unintended Consequences of GDPR*. The George Washington University, Washington D.C. 2020. 1-3. o.

rendszer mellett egy MI-vel foglalkozó Európai Testület létrehozásával megvalósuló közösségi együttműködés fogja biztosítani.

I.7. Összhang

A GDPR és AI Act horizontális jellege miatt teljes összhangra van szükség az olyan ágazatokra alkalmazandó hatályos uniós jogszabályokkal, amelyekben már alkalmaznak vagy a közeljövőben valószínűleg alkalmazni fognak nagy kockázatú MI-rendszereket.²⁰ Emellett kiemelt szerepet kell kapjon az összhang biztosításának az Európai Unió Alapjogi Chartájával, illetve az adatvédelemre, a fogyasztóvédelemre vonatkozó és más hatályos Uniós szabályokkal. Az adatvédelem kulcsfontosságú szerepet játszik abban is, hogy a polgárok bizalmát megőrizték az új technológiákkal szemben, illetve elkerüljék a polgárok jogainak és érdekeinek sérelmét. Így emiatt a javaslat célja, hogy ne módosítsa, hanem kiegészítse az általános adatvédelmi rendeletet és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet.²¹ Ennek ellenére a javaslat csupán egy szélesebb körű, átfogó intézkedéscsomag része, amely a fehér könyv tapasztalatai szerint kezeli a MI fejlesztése és használata által okozott problémákat, így ebből kifolyólag biztosítani kell a Bizottság által jelenleg is folyamatban lévő vagy tervezet kezdeményezései illetve más ágazati szabályokkal köztük más MI rendszerekre vonatkozó szabályok között is az összhangot. Ezért a kutatásom célja tehát, hogy feltérképezze és javaslatokat tegyen a keretek harmonizációjáról, így ezzel elősegítsem az MI fejlesztését az adatvédelmi szabályok tiszteletben tartásával.

II. GDPR szerepe és hatása az adatvédelemre: Előzmények, alapelvek, jogok és kötelezettségek

II.1. Alapfogalmak

A rendelet fogalmak szempontjából kevés újítást hozott és inkább a korábbi 95/46/EK számú adatvédelmi irányelv által már használt definíciókat vett át azzal az eltéréssel, hogy némi pontosítással és kiegészítéssel módosította azokat.

Ilyen fogalmak közül az adatvédelem szempontjából határozottan a legfontosabb a személyes adatok, amit a rendelet rendkívül tágan fogalmaz meg az által, hogy azt mondja „azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ” az azonosításról pedig, hogy a személy közvetlen vagy közvetett azonosítása is elegendő. Ilyen azonosításra alkalmas tulajdonságok közül a legfontosabbakat, mint például

²⁰ AI Act indoklás 1.2.

²¹ Vö. 20. jegyzet

név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező. Ezekről eltérően a rendelet külön meghatározza a genetikai-, biometrikus- és egészségügyi adat fogalmát, amelyeket együttesen különösen érzékeny személyes adatoknak tekintünk. Illetve hasonlóan kiemelt fogalom az adatkezelés, amelyet akként határoz meg, hogy „a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége” és ismételten példákat alkalmaz, mint például a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

MI-k szempontjából kiemelten jelentős lehet a későbbiekben, hogy kit tekintünk adatkezelőnek, illetve feldolgozónak, amelyet a könnyebb átláthatóság érdekében alább egy táblázatban szemléltetnek:²²

1. táblázat: Adatkezelő és adatfeldolgozó megkülönböztetése

Adatkezelő	Adatfeldolgozó
az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.	az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

Forrás: saját szerk.

Ez alapján az adatkezelő az adatfeldolgozóhoz képest egy sokkal tágabb kört jelent, amelybe a gyakorlatban sokszor adatokhoz hozzá nem férő személyek is beletartozhatnak, akik csak a GDPR rendelkezéseinek való megfelelést ellenőrzik és ezért ők az elsőszámú felelősök. Adatfeldolgozó pedig egy alárendelt pozícióban lévő személy vagy szerv, aki célt vagy eszközt

²² GDPR I. fejezet 4. cikk

nem határozhat meg, illetve az adatkezelő nevében és utasításai szerint kell eljárjon és neki mindig birtokába kerül személyes adat.

II.2. Adatkezelés alapelvei

A rendelet külön fejezetben határozza meg azokat az elveket, amelyek minden adatkezelés során érvényesülni 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 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 azok igazolására, így biztosítva az elszámoltathatóságot az adatkezelés teljes folyamata során („elszámoltathatóság”).²³

Ahogy korábban már említettem fő cél az érintettek védelme az adatkezelés során, amit az által ér el a rendelet, hogy az adatkezeléssel kapcsolatban rendkívül szigorú követelményeket támaszt az adatkezelővel szemben amellet, 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

²³ GDPR II. fejezet

adatkezelő számára, mert ez magába kell foglalja az érintettek megfelelő informálását az eljárással és jogaikkal kapcsolatban, saját szervezeti és működési szabályzatok kialakítását és pontos dokumentációt a teljes tevékenységével kapcsolatban egy esetlegesen felmerülő hiba elhárítása érdekében.

II.3. 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. A rendelet az érintettek jogainak vonatkozásában a korábbi irányelvi rendelkezésekből indul ki és azokat bővíti ki.

Az érintettek jogait három fő csoportba lehet sorolni az alapján, hogy a jog mely alapelv érvényesülését szolgálja.²⁴ 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. A 13-14. cikk tartalmazza a tájékoztatásra vonatkozó részletes szabályokat, mint például annak kötelező tartalmi elemeit, elsősorban írásban kell történnie, de kifejezett kérelem esetén van lehetőség szóbelire is, végül pedig legyen tömör, közérthető, könnyen és ingyenesen hozzáférhető, illetve megfelelő időn belül kerüljön rá sor. További átláthatósághoz kapcsolódó jog a tájékoztatáshoz sokban hasonló hozzáféréshez való jog. A legnagyobb különbség a kettő között, hogy ennek az esetben nemcsak az adatkezelés előtt, hanem annak folyamata során tud informálódni az adatkezeléssel kapcsolatban. Fontos más eleme ennek, hogy az érintett jogosult az adatai 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.²⁵

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

²⁴ Péterfalvi Attila – Révész Balázs – Buzás Péter: *Magyarázat a GDPR- ról*. Wolters Kluwer, Budapest 2018. (szerk.) 140-210. o.

²⁵ GDPR 2. szakasz

figyelembevételével az érintett jogosult arra is, hogy kérje hiányos személyes adatainak kiegészítését, beleértve a kiegészítő nyilatkozat útján történő kiegészítést 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 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.²⁶ A harmadik pedig az adatkezelés korlátozásához való jog, amelynek megfelelően a rendeletben meghatározott esetekben az érintett kérheti, hogy az adatkezelő korlátozza az adatkezelést.²⁷

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 következménye lehetséges következményei pont 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. Ellenben ezzel a jogával az érintett két konjunktív feltétel esetén élhet csak így, ha teljesen automatizált döntésről van szó vagyis mellőzve van minden emberi közreműködés és ez a döntés rá nézve valamilyen joghatással járna, illetve érintené őt. Emellett a rendelet említ kivételeket is, amelyek esetén nem lehet élni ezzel a joggal, ilyen, ha szerződés megkötése vagy teljesítése a kérdéses, uniós vagy tagállami jog teszi lehetővé vagy az érintett ehhez kifejezetten hozzájárult. Ez a jog a

²⁶ Vö. 24. jegyzet

²⁷ GDPR 3. szakasz

későbbiekben a mesterséges intelligenciák vizsgálatánál kiemelt helyzetbe kerül ezért a dolgozat előrehaladtával még említést teszek róla.

II.4. Kötelezettségek, avagy a mikro-, kis- és középvállalkozások kihívásai

Korábban már szót ejtettem arról a kötelezettségről, amely kiemelt jelentősége miatt több helyen is felmerül a rendelet rendelkezései között, hogy azok betartása elsődlegesen az adatkezelőt terhelik. Ez maga az elszámoltathatóság alapelve, amely nem csak az mondja ki, hogy az adatkezelő a felelős a megfelelésért, de azt is, hogy ennek a megfelelésnek az igazolására is képesnek kell lennie.²⁸ Ez az alapelv kiemelendő a többi közül mert rövid terjedelme ellenére a rendelet egészét áthatja és ebből adódik az adatvédelem „compliance” szemlélete. Ez a rendelkezés kötelezi arra az adatkezelőket, hogy belső irányelveket hozzanak létre, amelyek biztosítják a legjobb gyakorlatok alkalmazását és a jogi kötelezettségek teljesítését. Az adatkezelők kezébe adja a kockázatok azonosításának és kezelésének terhet, és arra ösztönzi őket, hogy munkatársaikat folyamatos képzésben részesítsék, annak érdekében, hogy tudatosan és jogszerűen járjanak el. Emellett ez a szabályozás megerősíti az átláthatóság és elszámoltathatóság elvét, amely elengedhetetlen a felelős adatkezelési gyakorlatok kialakításában. De a IV. fejezet általános kötelezettségeket rendező szakasza is további terheket ró az adatkezelőre:

1. Az adatkezelő figyelembe veszi az adatkezelés jelleget, hatókörét, körülményeit és céljait.
2. Az adatkezelés során értékeli a természetes személyek jogaira és szabadságaira jelentett kockázatot, melyek valószínűsége és súlyossága változó lehet.
3. Megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy biztosítsa és igazolja az adatkezelés összhangját a rendelettel.
4. Az intézkedéseket rendszeresen felülvizsgálja és szükség esetén naprakésszé teszi.²⁹

Ez különösen hangsúlyos mert, az új MI rendelettel és általánosan az MI-k szabályozásával kapcsolatosan az egyik legfontosabb kontra érv, hogy túlságosan nagy költségekkel jár a vállalkozások számára. Sok eltérő számítás készült a témában, amelyek sok esetben elfogultak, ezért teljes mértékben nem lehet bennük megbízni, de voltak olyan eredmények, amelyek több

²⁸ Vö. 23. jegyzet

²⁹ GDPR IV. fejezet 1. szakasz

ezer eurós terheket jelentenének éves szinten a befektetők számára. Ezek a terhek a nagy vállalatok esetében elenyészők, de a mikro-, kis- és középvállalkozások esetében sok esetben fenttarthatatlanok, amely azt jelentené, hogy az Európai Unió ezeknek a működését nehezítené meg nagy mértékben, amely mind a rendelet célkitűzéseivel, mind pedig az Unió általános céljaival ellentétes. Ha pedig ezeket a terheket úgy tekintjük, hogy már figyelembe vesszük a GDPR-ban már korábban meghatározott kötelezettségeket akkor ezek mikro-, kis- és középvállalkozások MI használatát teljesen képesek ellehetetleníteni.

Korábban a GDPR bevezetésének az egyik következménye az volt, hogy miután 2016 májusában hatályba lépett a rendelet és 2018 májusára kötelezővé vált annak alkalmazása a vállalkozások jelentős része erre nem volt képes ahogy ezt írja a Cisco Cybersecurity Series 2019-es januári jelentésében. Ebben jelentésben az látszik, 3.206 vállalkozás közül annak csak 59% jelentette azt, hogy a GDPR minden vagy majdnem minden rendelkezésének megfelel és 29% hogy 1 éven belül képes lesz ezeknek megfelelni.³⁰ Ez azt jelenti, hogy a meghatározott időtartam alatt a vállalkozások majdnem 2/3-a volt csak képes elérni a kötelezőként megállapított mércét. Ha pedig figyelembe vesszük az 1 éven belüli képes cégek számát is akkor látszik, hogy csak 2020-ra voltak csak képesek ezen az akadályon a vállalkozások jelentős része felülkerekedni. Ennek ellenére a rendelet sikeren könyvelhető el, hiszen rendkívüli mértékben felemelte az adatvédelem alapvető szintjét és megnövelte az adatvédelemmel kapcsolatos ismeretek átlagos mértékét. Sok esetben már a témában laikus személyek is tisztában vannak azzal, van egy rendelet, amely az adatvédelemért felelős. Ennek a következménye, hogy az adatvédelemre való igény, illetve az azzal kapcsolatos eljárás tisztázására vonatkozó igények száma rendkívüli mértékben megnőtt.³¹

II.5. Jogorvoslat, felelősség és szankciók

Az érintettek az adatkezelés során észlelt esetleges jogsértésekkel kapcsolatban az illetékes felügyeleti hatóságokhoz jogosultak fordulni jogorvoslat érdekében elsődlegesen. Ezeknek a független felügyeleti hatóságoknak kiemelt szerepet tulajdonítva a rendelet külön

³⁰ Cisco Systems (2019): Maximizing the value of your data privacy investments – Data Privacy Benchmark Study. Cisco Cybersecurity Series 2019, Data Privacy, 2019. január. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf (2024.10.30.)

³¹ Rákos Dóra: *A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében. Opuscula Iuvenum Excellentissima* 2019/2. szám, 32-35. o.

fejezetben rendelkeznek róluk és az együttműködésükről.³² Határokon átnyúló adatvédelmi esetekben az adatvédelmi hatóságok közösen járnak el. Magyarország esetében a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) tölti be ezt a szerepet az infotv. alapján.³³ De a hatóságok mellett nagy szerepe van az Európai Adatvédelmi Testületnek, amely olyan személyiséggel rendelkező uniós szerv, amelyet a tagállamok felügyeleti hatóságainak vezetői és az Európai Adatvédelmi biztosa alkot és fő feladata általános iránymutatás.³⁴

Amennyiben megállapításra került a jogsértés ténye abban az esetben ezek a hatóságok részben már említett módon a jogsértés figyelembevételével szankciókat alkalmazhatnak. Ezek közül az egyik legfontosabb szankció a közigazgatási bírság, melynek maximális mértékét a rendelet kevésbé súlyos és súlyos esetekben külön-külön meghatározza. De jogorvoslatra van lehetőség közigazgatási per keretében is és egy felmerült károkozás esetén a bíróságoknak joga van kártérítés meghatározására is. Ilyen per indítható a felügyeleti hatóságokkal szemben is amennyiben annak eljárásával szemben valamely jogos aggodalom merül fel.

II.6. GDPR alkalmazása mesterséges intelligencia esetében

A GDPR rendelkezései között már találhatóak utalások az automatizált rendszerekkel kapcsolatos előírásokra, de ezek az egyre gyorsabban fejlődő MI miatt további újragondolásra szorulnak. Az MI rendszerek által használt adatokat gyakran automatizált folyamatokban dolgozzák fel, és ez felveti az adatkezelés átláthatóságának és jogszerűségének kérdéseit. Emellett MI, különösen a gépi tanulás (machine learning) és a mélytanulás (deep learning) alapú rendszerek, jelentős mennyiségű adatot igényelnek ahhoz, hogy megfelelően működjenek és pontos előrejelzéseket tudjanak nyújtani. Ezek az adatok gyakran személyes adatokat is tartalmaznak, például demográfiai információkat, viselkedési adatokat, biometrikus adatokat, amelyeket több forrásból gyűjtenek össze. Ennek során figyelmet kell fordítani arra, hogy az adatok gyűjtése és feldolgozása során minden esetben megfeleljenek a GDPR előírásainak. Ez különösen fontos, mivel az MI rendszerek gyakran összetett és nehezen átlátható algoritmusokat használnak.³⁵

³² GDPR VI-VII. fejezet

³³ Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény V. fejezet

³⁴ GDPR. 139. preambulumbekzdés

³⁵ Stuart Russel – Peter Norvig: *Artificial Intelligence: A Modern Approach*. New Jersey, Pearson, 2016. 480-509. o.

A korábban említett alapelvek, így például az adatminimalizálás nagy kihívást jelentenek, mert első pillantásra ezek az elvek több szempontból is ellentmondanak a MI működési logikájának, amely jellemzően az adatok szabad és széleskörű felhasználására épül. Például egy arcfelismerő rendszer esetében szükséges lehet a biometrikus adatok gyűjtése, de az ilyen adatok kezelése különösen érzékeny, és szigorú szabályozás alá esik a GDPR szerint.³⁶ Másik különösen fontos alapelv a célhoz kötöttség, ami a MI esetében azért jelentős, mert ezek rendszerek képesek arra, hogy az adatokat új módon elemezzék, amelyeket az eredeti adatgyűjtés során nem vettek figyelembe. Az elvek betartása érdekében az MI rendszerek fejlesztésekor a "Privacy by Design" megközelítést kell alkalmazni, ami azt jelenti, hogy az adatvédelmet már a tervezési fázisban beépítik a rendszerbe, így biztosítva, hogy az megfeleljen a GDPR előírásainak. A GDPR egyik kulcsfontosságú követelménye az átláthatóság, amely megköveteli, hogy az adatkezelők világosan és érthetően tájékoztassák az érintetteket az adataik kezeléséről. A MI rendszerek átláthatósága különösen nagy kihívást jelent, mivel ezek a rendszerek gyakran „fekete doboz” módjára működnek, azaz Az MI rendszerek átláthatóságának javítása érdekében az adatkezelőknek törekedniük kell arra, hogy az algoritmusok működését érthetően kommunikálják az érintettek számára. Az MI rendszerek átláthatóságának javítása érdekében az adatkezelőknek törekedniük kell arra, hogy az algoritmusok működését érthetően kommunikálják az érintettek számára. Az automatizált folyamatok miatt veszélybe kerülhet az elszámoltathatóság elve, mivel a szükséges dokumentáció ki bővül a kockázatértékeléssel és rendszertervezési döntésekkel is, amellett, hogy az egyre nagyobb mennyiségű és gyorsabb folyamatok nehezebbé teszik a megfelelő minőségű dokumentációt.³⁷

³⁶ EDPB: *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. European Data Protection Board. https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf (2024.10.30.)

³⁷ Michael Veale – Lilian Edwards: *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*. In: Sophie Stalla-Bourdillon: *Computer Law & Security Review*. 34(2) Amsterdam, Elsevier 2018. 398-404. o.

III. A mesterséges intelligencia rendelet

III.1. A mesterséges intelligencia rendelet bevezetése

Az új rendelet létrehozását komoly előkészítő munka előzte meg hiszen az Unió folyamatos tevékenysége mellett ebben a témában számtalan független természettudománnyal, számítástechnikával, illetve jogtudománnyal foglalkozó szakember különféle kutatásai tették lehetővé. Erre jó példa már csak a MI definiálása hiszen rendkívül sok fogalom készült az elmúlt évek során, amelyek változatos irányból közelítették meg, ilyen a Norvég Adatvédelmi Hatóság (Datatilsynet) releváns jelentése ami úgy határozza meg az MI-t, hogy egy olyan rendszer, amely képes a saját tapasztalatai alapján tanulni és a megszerzett tudást eltérő helyzetekben alkalmazni összetett problémák megoldására.³⁸ Hasonló az Európai bizottság által 2018-ban kiadott „Mesterséges intelligencia Európa számára” című dokumentum amelyben az alábbiak szerint fogalmazták meg: „A mesterséges intelligencia intelligens viselkedésre utaló rendszereket takar, amelyek konkrét célok eléréséhez elemzik a környezetüket és – bizonyos mértékű autonómiával – intézkedéseket hajtanak végre”,³⁹ de ezt követően a bizottság által kifejeztem a MI-k tanulmányozására létrehozott magasszintű szakértői testület is új fogalmat hozott létre amely alapján „a mesterséges intelligencia alapú rendszerek olyan ember által tervezett szoftverek (és lehetőség szerint hardveres alapú rendszerek), melyek adott; meghatározott komplex célok elérése érdekében cselekszenek a fizikai vagy digitális dimenzióban, és elemzik környezetüket adatgyűjtés; az összegyűjtött rendszerezett vagy rendszertelen adatok értelmezése; tudásalapú érvelés vagy az információfeldolgozás által, a származtatott adatokból a legjobb, legmegfelelőbb cselekvést valósítják meg a meghatározott cél elérése érdekében.”⁴⁰

Emellett az Európai Unió az új rendelet megalkotása során nem kívánja a korábbi adatvédelmi szabályozó rendeletek hatályon kívül helyezését, hanem azokat figyelembe véve egy kiegészítő speciális jogszabály létrehozását kívánja megvalósítani.⁴¹ Ilyen rendeletek a

³⁸ Datatilsynet: *Artificial intelligence and privacy*. Report, January 2018. <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf> (2024. 10. 30.)

³⁹ A bizottság közleménye a közös európai adattér kialakítása felé COM (2018) 237 final

⁴⁰ The European Commission's High-Level Expert Group On Artificial Intelligence A Definition Of Ai: Main Capabilities And Scientific Disciplines. European Commission. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf (2024.10.30.)

⁴¹ AI Act 10. preambulumbekzdés

jelentősége miatt kiemelt GDPR, a 2018/1725 rendelete⁴², 2016/680 irányelv⁴³, illetve a 2002/58/EK irányelv.⁴⁴ Ezek bemutatása az általános adatvédelmi rendelet kivételével dolgozatomban meghaladja emiatt csak említés szintjén írok róluk.

III.2. Fogalommeghatározások

A rendelet fogalommeghatározásai között a korábban említett kiegészítő jelleg miatt összefüggések vehetők észre főleg a GDPR vonatkozásában, ezért a korábban leírtak alapján fogom az vizsgálatot végezni. A legfőbb fogalom a MI meghatározása amely a korábban említettektől eltérően végül olyan „gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet”. Ez a korábbi fogalommeghatározásokhoz képest egy lényegesen általánosabb megközelítés hiszen a hangsúly főként az alkalmazkodóképességen van és emellett, hogy különböző bemeneti információkból, maga által meghatározott módon hogyan tud egy számára meghatározott célt elérni. De a korábbiakkal szemben eltérés, hogy különböző szintekről tesz említést a rendelet, amely abból ered, hogy a megalkotása során kockázat alapú megközelítés mellett határoztak. Ennek érdekében a rendelet rögtön a MI után meghatározza a kárt egy egyszerű számításként a kár valószínűsége és annak súlya szerint.⁴⁵

További jelentős fogalmak a szereplők meghatározása, amelynek az esetében a rendelet a GDPR-hoz hasonlóan kettős megoldást alkalmaz és amelyeket a könnyebb értelmezése érdekében az alábbi táblázat segít:

⁴² Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről

⁴³ Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

⁴⁴ Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv)

⁴⁵ AI Act 3. cikk

2. táblázat: Szolgáltató és alkalmazó megkülönböztetése

Szolgáltató	Alkalmazó
olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely MI-rendszert vagy általános célú MI-modellt fejleszt vagy fejlesztett, és a saját neve vagy védjegye alatt – akár fizetés ellenében, akár ingyenesen – az MI-rendszert vagy az általános célú MI-modellt forgalomba hozza, vagy az MI-rendszert üzembe helyezi	olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely a felügyelete alá tartozó MI-rendszert használja, kivéve, ha az MI-rendszert személyes, nem szakmai jellegű tevékenység során használják

Forrás: saját szerk.

A két különböző definíció megalkotásából látszik, hogy a rendelet kiemelt hangsúlyt fektet arra, hogy a gyakorlatban ritka az az eset amikor ez a két személy egybe esik hiszen inkább az az elterjedt megoldás, hogy a jövőbeni alkalmazók egy MI létrehozása, üzembe helyezése és akár karbantartása érdekében a szakterületen jártasabb és MI rendszerekre specializálódott más vállalkozásokat bíznak meg.

Az adatok meghatározásakor a MI működése folytán több adatfajta is megkülönböztetésre került, amelyeket főként két csoportba lehet sorolni jellegük szerint. Az első csoport, amely a MI rendszer inkább informatikai szempontból jelentős tanulásához köthető, ilyenek a tanító-, validálási-, teszt- és bemeneti adatok. Második csoportba a dolgozatom szempontjából jelentősebb adatok tartoznak, amelyek maga az adat fajtája szerint kerültek meghatározásra, ilyen a biometrikus adat – amely a korábbi GDPR által már használt meghatározást vette át –, a személyes adatok és annak különleges kategóriái, amelyek a már említett rendeletek és irányelvek releváns bekezdéseire való hivatkozással lettek meghatározva. A korábbiakhoz képest viszont eltérés, hogy kiemelésre került az érzelemfelismerő rendszer, amely képes a „természetes személyek érzelmeinek vagy szándékainak a biometrikus adataik alapján történő azonosítására vagy kikövetkeztetésére”. Ebből arra lehet következtetni, hogy a személyes adatok korábbiakhoz képest más aspektusai is előtérbe kerülnek részben az MI-k megjelenésének részben pedig más társadalmi változások hatására, így olyan adatok is nélkülözhetlenné válnak, amelyek korábban nem voltak azok. Ilyenek lehetnek akár maguk az érzelmek és az arra vonatkozó információk is pontosan abból az okból mert, más korábban személyes adatként meghatározott információkhoz hasonlóan ezek is személyektől

elválaszthatatlanok. Ezt bizonyítja Andrew McStay egyik tanulmányában bemutatott eset is, ahol egy vállalat azt szerette volna felmérni, hogyan hat egy reklám az emberek érzelmeire, ezért létrehozott egy képzeletbeli kávémarkát. A reklám megtekintése után a cégnél rejtett kamerákkal rögzítették a vásárlók reakcióit, majd az arckifejezések elemzésével következtettek érzelmi állapotukra.⁴⁶ Az így gyűjtött adatok elemzése lehetőséget teremt arra is, hogy a preferenciák alapján az egyéneket manipulálják így ezek védelme indokoltá vált.

Összefoglalva az AI Act nem változtat a GDPR fogalommeghatározásain, ami nem is volt célja, hanem a korábbi fogalmakból emel ki a MI számára fontos elemeket. Így a célkitűzéseknek megfelelően nem hoz jelentős újításokat. Bár van néhány kisebb finomítás, mint az érzelmek kiemelése, de ez inkább bővíti csak a korábbi szabályozásokat mintsem módosítaná azokat.

III.3. MI rendszerek osztályozása

Az AI Act egyik leginnovatívabb és legjelentősebb eleme a MI rendszerek kockázati szintek szerinti osztályozása. Ez a rendszerek által jelentett kockázatokat és potenciális hatásokat veszi figyelembe, és ennek alapján határozza meg, hogy milyen szigorú szabályozási követelmények vonatkoznak rájuk. Az AI act négy fő kockázati szintet határoz meg.

Az első ilyen az elfogadhatatlan kockázatú rendszerek, amelyek teljes mértékben elfogadhatatlanok az Európai Unióban, amiatt mert megengedhetetlen mértékben veszélyeztetik, az emberi jogokat, jogállamiságot és más Unió értékeit. Ilyenek a korábban már említett társadalmi pontozási rendszerek, amelyek az egyének viselkedését állami vagy magánintézmények értékelik és büntetik. Ennek célja, hogy elkerüljék a kínai „social credit” rendszert, amelyben a polgárokról nyilvántartott különböző adatok alapján döntenek számos kérdésben, mint például a számukra nyitva álló hitel lehetőségekről, állami támogatásokról, illetve akár az oktatásban való részvételről.⁴⁷ Ehhez hasonló tiltott rendszer még a rejtett manipulációs rendszerek, amelyek különböző személyes adatok segítségével próbálják irányítani a felhasználók döntéseit, hogy azok például tudat alatt egy olyan terméket vásároljanak, amelyet máskülönben nem vennének meg vagy esetleg olyan szavazatot adjanak le amit korábban nem tettek volna. De a személyes adatok tekintetében az egyik legfontosabb

⁴⁶ Andrew Mcstay: *Emphatic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)*. Big Data and Society. 3. o.

⁴⁷ Kollár Csaba: *Kína és a társadalmi kredit rendszere*. REAL - az MTA Könyvtárának Repozitóriuma. https://real.mtak.hu/118296/1/079-097_Kollar.pdf (2024.10.30.)

rendszerek, amelyek képesek nyilvános helyen valós időben biometrikus azonosításra, vagyis különösen érzékeny személyes adatok felhasználásával lehetővé teszik például személyek nyomkövetését vagy akár lehallgatását. Ezek az adatok már a GDPR-ban szigorított védelemre méltóként voltak meghatározva és az új rendelet is szigorúan tiltja az ilyen MI rendszerek alkalmazását kevés kivétel meghatározásával, ilyen eset amikor súlyos bűncselekmények megelőzése érdekében alkalmazzák, de ekkor is kizárólag hatósági engedéllyel lehetséges.

Második csoport a magas kockázatú rendszerek, amelyek jelentős hatással lehetnek az emberek életére, mert egészségügyben, oktatásban, munkaerőpiacon vagy a közszolgáltatások terén kerülnek alkalmazásra és így az előbb ismeretekhez hasonlóan különösen érzékeny adatokhoz férhetnek hozzá, emiatt szigorú adatminőségi követelmények, dokumentációs kötelezettségek és auditálási előírások vonatkoznak.

Harmadik a korlátozott kockázatú rendszerek, amelyek már kevésbé szigorú korlátozások alá esnek. Ide tartoznak többek között a „chatbotok”, ügyfélszolgálati rendszerek, amelyek MI-t használnak. Ezek esetében egyértelművé kell tenni a felhasználók számára, hogy a termék vagy szolgáltatás MI rendszerrel kommunikál és biztosítani az emberi beavatkozást. Ennek a csoportnak az alacsony veszélyeztetettségét az indokolja, hogy a szolgáltatás fontos adatokhoz ritkán vagy egyáltalán nem fér hozzá és a felhasználók általi engedélyezéstől nagy mértékben függ.

Negyedik és egyben az utolsó csoport a minimális kockázatú rendszerek, amelyeknek a legalacsonyabb előírásoknak kell csak megfelelni. Ilyen lehet egy MI-vel működő spam-szűrő, automatikus szövegkiegészítő, illetve egyes játékokban alkalmazott rendszerek. Ezeknek az esetében szinte kizárt, hogy bármilyen személyes adathoz férjenek hozzá ezért elegendő az alapvető adatvédelmi és biztonsági rendelkezéseknek megfelelni.

Ebből arra lehet következtetni, hogy csoportosítást az adatvédelmi elvekre (is) tekintettel alkották meg, mivel jelentős mértékben befolyásolja egy MI rendszer kockázati besorolását, hogy az milyen személyes adatokhoz fér hozzá, illetve azokat milyen döntések meghozatalára használhatja fel. Emelet kiemelten fontos a kockázat meghatározásánál, hogy elkerülhető-e az adott rendszer használata, mint egy spam szűrő esetében vagy pedig szükséges, mint például a közigazgatásban megjelenő rendszerek, amelyek az elképesztően nagy adatmennyiségek miatt az adatok értékelése ember által már lehetetlenné vált.

III.4. Kiberbiztonság és az adatvédelem

Magától értetődően a magas kockázatú rendszerek szigorúbb biztonsági előírásokat igényelnek, mint az alacsonyabb kockázatú rendszerek. Ezek az előírások több szinten is

biztosítják, hogy a felhasználók adatai és jogai védve legyenek. Ilyen előírások találhatóak a kiberbiztonság biztosítása érdekében, amely alapvető fontosságú az MI rendszerek esetében ezért az a rendelet előírja, hogy magas kockázatú rendszerek esetében szigorú kiberbiztonsági szabályoknak kell megfelelni, amibe beletartozik a titkosítás, a hozzáférés-szabályozása, és az adatvesztés elleni védelem. Cél, hogy minimalizálni tudják az adatvédelmi incidensek előfordulásának kockázatát, például egy esetleges hackertámadás vagy más adatlopás lehetőségét. Ezen előírások betartása kulcsfontosságú ahhoz, hogy az MI rendszerek megfeleljenek a GDPR adatvédelmi követelményeinek is.⁴⁸ Ezenfelül a rendelet előírja a folyamatos megfelelés és auditálás követelményét a magas kockázatú rendszerek számára. Ez azt jelenti, hogy az ilyen rendszereknek nem csak a kezdeti beüzemelés során kell megfelelniük az előírásoknak, hanem folyamatosan, a rendszer teljes élettartama alatt. Az auditálás során rendszeresen ellenőrizni kell, hogy a rendszer megfelel a követelményeknek és megfelelően kezeli-e a személyes adatokat. Ez az előírás hivatott biztosítani, hogy a rendszerek képesek legyenek naprakészek maradni a legmodernebb fenyegetésekkel szemben is.

III.5. AI Act Összefoglalás

Az AI Act és a GDPR közötti kapcsolat az adatvédelem területén rendkívül fontos, amikor MI rendszerekről van szó. Az AI Act részletesebben szabályozza azokat az adatvédelmi előírásokat, amelyeket a GDPR általánosan megfogalmaz. Különösen a magas kockázatú MI rendszerek esetében ad pontos irányelveket. Ez az új szabályozás biztosítja, hogy a MI ne csak technológiailag fejlődjön, hanem jogilag is megfeleljen a felhasználók adatvédelmi jogainak. Az AI act és a GDPR együttműködése garantálja, hogy a felhasználók személyes adatai a lehető legjobb védelemben részesüljenek a digitális korban, miközben lehetővé teszik az MI rendszerek további fejlesztését és használatát. Az AI act célja, hogy ne csupán egy új szabályozást hozzon létre, hanem integrálja és konkretizálja a GDPR rendelkezéseit, így egy átfogó és következetes rendszert biztosít a mesterséges intelligenciával kapcsolatos jövőbeni kutatásokhoz és alkalmazásokhoz.

⁴⁸ Robert Walters - Marko Novak: *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Springer Nature Singapore, Singapore 2021. 71-93. o.

IV. Következtetések a két rendelet viszonyával összefüggésben

IV.1. Alapelvek teljesülése

A két rendelet, 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, tisztességességére és jogszerűségére helyezi a hangsúlyt. Ezzel szemben az AI Act célja a mesterséges intelligenciával 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.

IV.1.1. Jogszerűség, tisztességes eljárás és átláthatóság

A GDPR által meghatározott adatkezelés jogszerűségének hat jogalapja – beleegyezés, szerződés, jogi kötelezettség, létfontosságú érdekek, közérdek és jogos érdekek – az AI Act keretein belül is érvényes, amikor személyes adatokat feldolgozó MI rendszerekről van szó. A jogalapok átemelése biztosítja, hogy az MI rendszerek működése összhangban legyen a meglévő adatvédelmi normákkal, ezzel elősegítve a jogszerű adatkezelést és a felhasználók jogainak védelmét. És amíg az AI Act fejezetei között nem találunk konkrét rendelkezést a tisztességes eljárás elvére, mivel a GDPR elveire épít több szakaszban – mint az MI fejlesztése és alkalmazása esetén – utal a rendelet az elfogultság és diszkrimináció tilalmára. Az átláthatóság elvét a rendelet azáltal próbálja meg implementálni, hogy előír egy átláthatósági minimumot, ami minden MI esetében alkalmazni kell, emellett pedig a kockázatalapú megközelítéséhez hasonlóan szigorítja a kötelezettségeket a magasabb kockázatú MI-k esetében. Ezek a kötelezettségek eleinte kimerülnek egy pusztán tájékoztatásban, amelynek keretében felvilágosítják az érintettet, hogy éppen egy MI alapú rendszert alkalmaz. A magasabb kockázatú rendszerek esetében előírás lehet, hogy tájékoztatást adjanak arról, hogyan használják fel az adatokat, valamint részletes információkat a döntéshozatali folyamatokról. De az átláthatóságról kiemelt jelentősége miatt később külön szót ejtek.

IV.1.2. Célhoz kötöttség és adattakarékosság

A GDPR által meghatározott elveket, miszerint a személyes adatokat meghatározott és jogszerű célokra kell gyűjteni, és csak az adott célhoz szükséges mértékben lehet azokat felhasználni az AI Act egy lépéssel tovább szigorítja. A célhoz kötöttség elve magas kockázatú

MI rendszerek esetében azáltal, hogy tisztázza a meghatározott és jól dokumentált célok szükségességét

IV.1.3. Pontosság

Az AI Act a pontosság elvét főként az MI rendszerek fejlesztésének kockázatai miatt kiegészíti azzal, hogy előírja a magas kockázatú MI rendszerek használata esetében, hogy biztosítani kell az adatok magas színvonalát és a torzítástól mentességét, hogy így megelőzze a diszkriminációt.

IV.1.4. Korlátozott tárolhatóság

A GDPR-hoz képest az új rendelet nem vezet be további követelményeket. Ez alapján a korábbi rendelkezéseket kell alkalmazni, amely felvethet néhány aggályt. Ha az a rendelkezés, amely alapján a személyes adatokat csak annyi ideig lehet tárolni, ameddig a cél a meghatározott célok eléréséhez szükséges felveti a kérdést, hogy mit kell tenni az adatokkal ez után. A kérdés egyértelműnek tűnhet hiszen a legegyszerűbb válasz, hogy törölni kell azokat, de ebben az esetben felmerül egy újabb kérdés. Mi történik a rendszer hatékonyságával? Hiszen az MI rendszerek lényege abban rejlik, hogy az idő előrehaladtával, ahogyan a bevitt adatok és a meghozott döntések száma növekedik egyre pontosabban képes dolgozni ez a rendelkezés viszont ezzel ellentétes. De akár felmerülhet az is megoldásként, hogy az adatokat nem kell vagy legalábbis nem minden esetben kell törölni elég azok anonimizálása.

IV.1.5. Integritás és bizalmas jelleg

Mind a két rendelet kiemeli az adatvédelem fontosságát az adatkezelés teljes időtartama alatt ezért előírják a megfelelő technikai és szervezeti intézkedések alkalmazását. Ennek megfelelően a GDPR már korábban is támogatta, hogy a különböző szervezetek saját belső szabályokat alakítsanak ki annak érdekében, hogy a személyes adatok kezelése megfeleljen az adatvédelmi előírásoknak. Ezek a belső szabályok segítenek a vállalatoknak a megfelelő adatvédelmi gyakorlatok kialakításában és biztonsági intézkedések fenntartásában. Így képesek figyelembe venni az adott szervezet sajátos igényeit és az általuk kezelt adatok jellegét, valamint a kezeléssel járó potenciális kockázatokat. Ehhez hasonló rendelkezést találunk az AI Act-ben, ami a MI jártasságra helyezi a hangsúlyt így az MI rendszer szolgáltatóknak és alkalmazóknak biztosítaniuk kell, hogy személyzetük és a nevükben az MI rendszereket működtető egyéb személyek rendelkezzenek megfelelő MI-ban való jártassággal. Ennek

érdekében figyelembe kell venniük ezen személyek szakmai tapasztalatát, képzettségét, valamint azokat a körülményeket, amelyek között az MI rendszereket működtetik. De más biztonsági rendelkezés, amelyet találunk a GDPR-ban a kockázatértékelés, hogy az adatkezelők felismerjék a személyes adatok kezeléséből eredő potenciális veszélyeket és meghatározzák azokat az intézkedéseket, amelyekkel a kockázatokat minimalizálni lehet. Az AI Act erre építve a MI sajátosságainak figyelembevételével, hogy elkerüljék a lehetséges torzulást a tanuló adatokban vagy akár az adatok illetéktelen módosítását további megelőző kockázatkezelési rendszert vezet be a magas kockázatú MI rendszerek esetében. Ilyen az ismert, valamint észszerűen előre látható kockázatok azonosítása és elemzése, folyamatos megfigyelés és ellenőrzés – mind az adatok torzulása mind pedig a kiberbiztonsági veszélyekkel szemben –, az emberi felügyelet

IV.2 A kockázatalapú megközelítések párhuzamai

A kockázat alapú megközelítés mind a két rendelet szerves részét képezi, ezért nem lehet elmenni a fölött, hogy megvizsgáljam az az AI Act mennyire támogatja a GDPR alapján meghatározott adatkezelési követelmények kockázat szerinti szigorításának megvalósítását. Az AI Act számos módon kiegészíti a GDPR előírásait főként a magas kockázatú MI rendszerek adatkezelési követelményei esetében. Így bár kiterjedt szabályokat fogalmaz meg a MI által kezelt adatokkal kapcsolatban, alapvetően kiegészíti, és nem helyettesíti a GDPR által előírt elveket, különösen a kockázatok megfelelő kezelésében. Emiatt az AI Act egyfajta kockázat alapú intézkedési csomagot hoz létre a GDPR kockázatkezelési megoldásaihoz igazodva. Az egyik lényeges kérdés tehát, hogy az AI Act valóban képes-e ezzel az adatkezelési csomaggal az adatkezelési gyakorlatot a GDPR szerinti elvek alapján optimalizálni és biztosítani, hogy a fokozott kockázatú helyzetekben is betarthatók legyenek az adatvédelmi követelmények.

A GDPR esetében a kockázatalapú adatkezelés kiindulópontja, hogy az erre vonatkozó adatkezelői döntések már a jogalap megválasztásánál megjelennek, mint például az érdek mérlegelés körében, ahol az eljárás elején döntést hoznak a szükségesség és arányosság mércéjével az intézkedés indokoltságáról és megfelelőségéről. Ez kivételesen igaz amikor a jogalként a jogos érdeket határozzák meg hiszen ilyenkor a megfelelő egyensúly egyszerre szolgálja a GDPR céljait és döntések rugalmasabb meghozatalát is. Az AI Act ebből a megközelítésből indul ki főleg a magas kockázatú MI-k esetében. A megelőző intézkedéseket már a MI rendszerek tervezési szakaszaiban megkezdik, illetve beépítik. Ez a kötelezettség onnan ered, hogy a rendszert ne lehessen más, az eredeti céljaival összeegyeztethetetlen szándékkal alkalmazni, például személyes adatok illetéktelen feldolgozására vagy az érintettek

jogaival ellentétes felhasználásra és így csökkentse az adatfeldolgozási kockázatokat. A különbségek legfőképpen az adatvédelmi hatásvizsgálatok tükrében a legfeltűnőbbek. Ameddig GDPR esetében az adatvédelmi hatásvizsgálatok a magas kockázatú adatkezelések előzetes értékelését írja elő, addig az AI Act ezen túl teljes MI rendszer kockázatkezelési politikát ír elő. Ebbe beletartozik a rendszer teljes életciklusára működési környezetének folyamatos megfigyelése és felügyelete is

IV.3. Adatvédelmi hatásvizsgálat és az alapvetőjogi hatásvizsgálat viszonya

A GDPR előírja, hogy új technológiák, beleértve a MI használatával végzett személyes adatok kezelését, adatvédelmi hatásvizsgálatot (DPIA) kell végezni az egyének jogait és szabadságait érintő potenciális kockázatok felmérésére.⁴⁹ A GDPR nemcsak a DPIA elvégzésére kötelező kategóriákat határoz meg, hanem felhatalmazza és támogatja az Adatvédelmi Hatóságokat is, hogy további kategóriákat határozzanak meg, amelyek esetében kötelező a DPIA elvégzése. Ezzel párhuzamosan az AI Act a magas kockázatú MI technológiákat a lényeges jogokhoz, a demokráciához és a társadalomhoz való kockázati szintjük szerint osztályozza, és megköveteli egy Alapvetőjogi Hatásvizsgálat (FRIA) elvégzését is.⁵⁰ Jelentős kérdés tehát, hogy hol és hogyan szükséges a DPIA, valamint mi a kapcsolata az AI Act által megkövetelt kockázatelemzéssel.

A két rendelet kockázatalapú megközelítésből eredően a kockázatok taxatív meg nem határozott kategóriához kötik a hatásvizsgálatok elvégzését. A GDPR apaján az adatvédelmi hatásvizsgálat ex-ante jellegű intézkedés, a személyes adatok feldolgozói számára, amikor az adatok feldolgozása magas kockázattal jár a természetes személyek jogaira vagy szabadságaira nézve.⁵¹ A GDPR emellett utal az új technológiák használatára, mint a DPIA jogalapja. Ez a rendelkezés három feltétellel magába foglalja a MI rendszereket is. Először is, ha a személyes adatok feldolgozása automatizálást foglal magában, amely természetes személyek rendszerszintű és széleskörű értékeléséhez vezet, jogi következményekkel járva. Másodszor, nagyszabású feldolgozás esetén, amely különleges kategóriákat vagy büntetőjogi döntéseket érint. Harmadszor, nagyszabású, rendszerszintű megfigyelés esetén, amely nyilvánosan hozzáférhető területet érint. A három fő feltétel mellett kerültek további kategóriák meghatározva egyedi módon tagállamonként és olyan Európai Gazdasági Térséghez tartozó

⁴⁹ GDPR 35. cikk

⁵⁰ AI Act 27. cikk

⁵¹ GDPR 35. cikk

államonként, amelyekre hatályos a GDPR. Ezzel szemben az AI Act a III. mellékletében meghatározott magas kockázatú MI rendszerek, ha azok társadalmi alapjogokat, a demokráciát vagy az egyének szabadságát és jogait érintően jelentenek magas kockázatot. Ez alapján öt faktor kell vizsgálni a kockázatok számításakor megállapítani⁵²:

1. Terület vagy szektor, pl. oktatás;
2. Cél, pl. vizsgák értékelése;
3. Képesség vagy használt MI technika, pl. információkeresés;
4. MI üzemeltetője, pl. iskola/univerzitás; és
5. MI alany, pl. diákok.

Ez az öt faktorból álló keretrendszer hasznos annak megértésében, hogy milyen információkra van szükség annak értékeléséhez, hogy egy MI magas kockázatúnak minősül-e az AI Act III. mellékletének rendelkezései szerint.

Miután a FRIA alkalmazása az AI Act alapján egyértelmű ezért a fennmaradt kérdés, hogy mely esetekben van szükség DPIA elvégzésére. Az Institute of Electrical and Electronics Engineers (IEEE) egy átfogó kutatást készített⁵³, ahol alapul vették a GDPR-t, az Európai Adatvédelmi Testület iránymutatásait és az államok adatvédelmi hatóságai által előírt feltételeket. Ezek alapján 94 különböző feltételt találtak, amely DPIA jogalapja lehet. Érdekes megállapítás, hogy a MI bármilyen használata esetén DPIA szükséges Ausztriában, Dániában, Németországban, Görögországban és a Cseh Köztársaságban. De ezek között a leggyakoribb feltételek a (nagy léptékű) kommunikációs és helymeghatározási adatok kezelése (23 ország), a munkavállalói tevékenységek (nagy léptékű) feldolgozása (19 ország) és a joghatásokkal járó adatkezelés, például szolgáltatásokhoz való hozzáférés vagy azok kizárása (12 ország). A specifikusabb tevékenységek közé tartozik a pénzügyi adatok (nagy léptékű) feldolgozása (amit öt tagállam említ) vagy az iskolai elektronikus megfigyelés (amit két tagállam említ), amelyek jóval pontosabb adatkezelési típusokat képviselnek. Ezeknek a feltételeknek a kulcselemét később a könnyebb összehasonlítás végett 5 tényező alapján rendszerezték:

1. A feldolgozási tevékenység célja;

⁵² D. Golpayegani - H. J. Pandit - D. 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.

⁵³ Tytti Rintamäki et. al.: *High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications*. Exeter, European Journal of Law and Technology, 2023. 1-20. o.

2. Személyes adatok – különösen, ha érzékeny vagy különleges kategóriába tartoznak-e, pl. egészségügyi adatok vagy bűncselekmények és vétségek;
3. Adat alanyok – különösen, hogy sebezhetőek-e, pl. gyermekek, kisebbségek;
4. Specifikus technológiák bevonása – különösen, hogy innovatívok és tesztelés alatt állnak-e, pl. MI; és
5. Feldolgozási kontextus – mint például az automatizált döntéshozatal, profilalkotás bevonása, és hogy a feldolgozás jogi hatásokat gyakorol-e az adat alanyra.

Ezeket összehasonlították az AI Act III. mellékletében meghatározott 25 (8 csoport és ezek alcsoportjai) magas kockázatú MI meghatározással, amelyek közül megvizsgálták, hogy melyek azok, amelyekre a GDPR hatálya feltétlen vagy feltételesen kiterjed mert személyes adatokkal érintkeznek. Így több eredményt is kaptak a kutatásban, de talán a jelen téma szempontjából a legfontosabb, hogy a GDPR kifejezetten alkalmazandó eseteiben, a III. melléklet 25 alpontjából 23 előírja az DPIA kötelező elvégzését. Ez bizonyítja, hogy jelentős átfedés van az AI Act III. mellékletének magas kockázati besorolása és a GDPR DPIA követelményei között, vagyis általánosan mennyire van szorosan integrálva van a GDPR alkalmazása az AI Act kockázati besorolásában.

Miután, hogy tisztáztuk, mikor szükséges DPIA-t és FRIA-t végezni, a következő lépés a hatásvizsgálatok konkrét folyamatának, illetve egymáshoz való viszonyuknak az elemzése. Ebben a kérdésben is segítségemre van az IEEE által végzett kutatás, ami a véleményemmel azonos eredményre jutott.⁵⁴ A DPIA és az FRIA egyaránt kötelezően megelőző jellegű vizsgálatok, amelyeket a MI rendszer bevezetése előtt kell elvégezni. De a DPIA akár az életciklus elején AI fejlesztés korábbi fázisaiban is elvégezhető. Mivel a DPIA és a FRIA között számos hasonlóság van, az egyik lényeges kérdés a FRIA alkalmazásakor az, hogy milyen módon lehet összehangolni a meglévő hatásvizsgálatokat. Az AI Act kifejezetten lehetővé teszi, hogy a DPIA az FRIA követelményeit „kiegészítve” újra felhasználásra kerüljön.⁵⁵ Ezzel a MI fejlesztési láncolat szereplői közötti információmegosztással jelentős mértékben csökkenthetőek a vagyoni és személyzeti terhek mivel ezzel nő az átláthatóság, ami miatt könnyebben elkerülhetőek a redundáns folyamatok így megkönnyítve az erőforrások kezelését. Ebből egyértelműen látszik, hogy a FRIA csak a III. melléklet néhány felhasználási esetén szükséges, a GDPR értelmében a DPIA-ra az esetek túlnyomó részében továbbra is szükség van, és a DPIA hatóköre magában foglalhatja az FRIA által érintett jogokat és szabadságokat.

⁵⁴ Vö. 53.

⁵⁵ AI Act 27. cikkének (4) bekezdés

Miután DPIA esetében az AI Act nagy mértékben visszanyúl a GDPR rendelkezéseihez, ezzel együtt jár, hogy a tagállamok között jelentős eltérés lehet a DPIA alkalmazásának feltételeiben, ami nagymértékben bonyolíthatja a DPIA hatékony alkalmazását tagállamok közötti esetekben. Ezen kihívások enyhítésében a későbbiekben lehet segítséget nyújthatnak az AI Act FRIA-ra vonatkozó rendelkezései, ha a gyakorlat ezt képes megvalósítani.

IV.3. Átláthatóság az MI-rendszerekben

Az európai adatvédelmi szabályozás egyik alapkövetelménye az átláthatóság, amely alapelveként végigvonul a teljes jogi keretrendszeren. Célja, hogy az adatkezelési folyamatok átláthatók maradjanak, biztosítva az elérhető és értelmezhető információhoz való hozzáféréssel az érdekvédelmi eszközök gyakorlását. De a gyakorlat szempontjából nem elhanyagolható, hogy mit értünk pontosan átláthatóság alatt főleg különösen olyan esetekben, amelyekben több jogszabályt kell párhuzamosan alkalmazni és azok részben eltérnek. Ennek a kérdésnek az eldöntésében segít nekünk a GDPR 39. preambulumbekzdése.⁵⁶ 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.⁵⁷ Így ezek értelmezése érdekében az Európai Adatvédelmi Testület iránymutatásait célszerű megvizsgálni. A több kiadott iránymutatás között, amely az átláthatóság témájával foglalkozik kiemelt jelentőséggel bír a 2018-ban kiadott.⁵⁸ Ez alapján az átláthatóság megköveteli, hogy az adatkezelők világos és érthető, jogi zsargontól mentes információkat adjanak az érintetteknek, amelyek pontosak, naprakészek és könnyen hozzáférhetők. Hiszen ezeknek a jogoknak a hatékony érvényesítése erősen függ a tájékoztatás által biztosított átláthatóságtól. Az érintettek csak akkor tudják érvényesíteni jogaikat, ha megfelelő információval rendelkeznek az adatkezelési tevékenységekről.⁵⁹ Ezeket a feltételeket új technológiák esetén is biztosítani kell annak ellenére, hogy ezek új nehézségeket teremtenek az átláthatóság gyakorlati megvalósíthatósága ellen. Emiatt az EDPD

⁵⁶ GDPR 39. preambulumbekzdés

⁵⁷ GDPR 12. Cikk

⁵⁸ EDPB: Guidelines on Transparency under Regulation 2016/679

⁵⁹ Mahieu René - Jef Ausloos: *Harnessing the collective potential of GDPR access rights: towards an ecology of transparency*. Berlin, Internet Policy Review 3.4, 2020.

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 a korábbiakban említettek alapján gyakran „fekete dobozoknak”.⁶⁰ Emiatt mostanra már elsődleges fontosságú, hogy az AI Act, hogyan képes a GDPR sokszor bizonytalan értelmezésű átláthatósági követelményeinek megfelelni és azokat az MI-k sajátosságaira tovább vezetni.

Az MI technológiai megoldások gyakran bonyolult adatkezelési folyamatokat foglalnak magukban, amelyek a „black box” hatás miatt nehezen átláthatóak még a technológia fejlesztője vagy üzemeltetője számára is.⁶¹ Ha ezek a rendszerek személyes adatokat is kezelnek, akkor a jogi megfelelés biztosítása érdekében egyszerre szükséges megfelelni a fent ismertetett átláthatósági követelményeknek, valamint az algoritmikus döntéshozatalra vonatkozó egyéb szabályozásoknak. Az európai jogalkotó ezért fontosnak tartja szabályok megalkotását az átláthatóság növelésére, különösen a természetes személyek számára érthetetlen vagy túl komplex MI-rendszerek esetében. Ezért az AI Act 47. preambulumbekkezdése előírja, hogy a magas kockázatú MI-rendszerek esetében megfelelő dokumentációval és egyértelmű tájékoztatással kell ellátni a felhasználókat, hogy megértsék és helyesen alkalmazzák a rendszereket.⁶² 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.⁶³ 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 határoza meg.⁶⁴ A minimumkövetelmények megfogalmazása során részben az adatvédelmi jogban már meglévő elemeket integrál, amelyek a felhasználók számára egyértelmű, hozzáférhető, és tömör információkat biztosítását célozzák. Ezen túlmenően viszont új követelményeket is felállít, amelyek a technológiai sajátosságokra és a felmerülő problémákra vonatkoznak. Ezek a követelmények előírják egy olyan dokumentum (használati utasítás) létrehozását, amely az

⁶⁰ Vö. 6. jegyzet

⁶¹ Frank Pasquale: *The Black Box Society: The Secret Algorithms Behind Money and Information*. Harvard University Press, Cambridge 2016. 59-100. o.

⁶² AI Act 47. preambulumbekkezdés

⁶³ AI Act 13. cikk (1) bekezdés

⁶⁴ AI Act 13. cikk (2)-(2) bekezdés

átláthatóság és 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.⁶⁵ 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.⁶⁶

IV.4. Érintetti jogok biztosítása MI környezetben

Végül a kutatásomban vizsgált utolsó kérdés a két rendelet viszonyában az érintetti jogok biztosítása. Mivel a GDPR az érintetti jogok széles körét írja elő és a MI rendszerek adatkezelési műveleteinek komplexitása kihívást jelenthet a jogok gyakorlásában.⁶⁷

A helyesbítés joga a GDPR alapján feljogosítja az érintetteket, hogy javítást kérjenek a pontatlan személyes adataikkal kapcsolatban. A MI rendszerekben, ahol adatokat gyakran automatikusan dolgozzák fel és használják fel, ennek biztosítása nagy kihívást jelenthet. A helyesbítés korlátozottan értelmezhető olyan MI környezetben, ahol az adatokat folyamatosan újra feldolgozzák vagy aggregálják, és az AI Act nem biztosít explicit mechanizmusokat az ilyen korrekciós jogok hatékony gyakorlására. A Tiltakozáshoz való jog lehetővé teszi az érintettek számára, hogy kifogással élhessenek adatainak feldolgozásával szemben. Az AI Act célja ezekben az esetekben, hogy biztosítsa az átláthatóságot, amely a korábban megállapítottak alapján kétes értelmezésű és a dokumentációt. De a rendeletben nem találunk rendelkezést, ami teljes mértékben garantálná az érintettek tiltakozását az adataik feldolgozása ellen.

A tájékoztatás joga a tiltakozás jogához hasonlóan az átláthatóságot hivatott biztosítani, de az is felvethető, hogy e kötelezettségek különállóságának megítélése kérdéses, mivel egy olyan értelmezés is létezik, amely szerint minden tájékoztatási kötelezettség az átláthatóságot elősegítő intézkedésként fogható fel. A tájékoztatás konkrét mechanizmusainak hiányában az érintettek nehezen tudják gyakorolni információs jogukat, hiszen nincs kiindulópontjuk, amely

⁶⁵ Varošanec Ida: *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.

⁶⁶ Busuioc Madalina - 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.

⁶⁷ GDPR III. fejezet

alapján biztosítani tudnák a jogérvényesítést. Az AI Act a preambulum részében ugyan több helyen is kiemeli, hogy célja az érintettek bizalmának növelése a MI rendszerekkel szemben, de miután az információhoz való hozzáférés személyre szabott módon történő biztosítása továbbra is jelentős kihívás így ebből a szempontból ezt a célkitűzést nem sikerült kielégítő módon elérni.

Ezek alapján egyértelműen megállapíthatom, hogy az átláthatósághoz hasonlóan az AI Act a GDPR-ban meghatározott követelményeket csak részben képes megvalósítani a MI technológia területén. A rendelet egészében találunk rendelkezéseket, melyek az érintetti joggyakorlást hivatottak elősegíteni – magas szintű dokumentáció, használati utasítás – de ezek a sokszor általános jellegű előírások a korábbi GDPR által kialakított érintett központú rendszer szintjét nem érik el.

V. Konklúzió

Az AI Act jelentős előrelépés a MI technológia kodifikációjában. A rendelet célja, hogy biztosítsa a felhasználók védelmét és a jogszerű adatkezelést, amely a GDPR alapelveivel is összhangban van. A rendelet kockázat alapú megközelítése kiemelkedően jó döntés, mivel ez nagyban képes elősegíteni a GDPR kereteihez való illeszkedést. A GDPR már eddig is a kockázatok azonosítására és kezelésére épült, hangsúlyozva az adatkezelés jogszerűségének és átláthatóságának fontosságát. Ezen megközelítés előnye, hogy nem csupán a szabályozás szigorúságát növeli, hanem rugalmasságot is biztosít, lehetővé téve a vállalkozások számára, hogy az alkalmazott AI rendszerek kockázati szintjének megfelelően alakítsák ki saját belső szabályzataikat és gyakorlatukat. Tehát ez a megközelítés nem csak jogi megfelelési szempontból kedvező, de hozzájárul az innováció ösztönzéséhez is. Több a rendelet által előírt intézkedés, mint például a DPIA és a magas kockázatú rendszerekre vonatkozó fokozott kötelezettségek képesek elősegíteni a technológiával szembeni bizalom növelését. Ugyanakkor a rendelet több helyen nem, vagy csak részben felel meg a GDPR elvárásainak. Például a GDPR és AI Act átláthatóságra vonatkozó rendelkezései többértelműek, és a lehetséges értelmezések néha ellentmondásosak is. Mit takar pontosan az átláthatóság fogalma? Jelenti-e az információk érthetőségét és értelmezhetőségét, vagy csupán azt, hogy betekintést nyerhetünk a folyamatokba? Az AI Act kontextusában az átláthatóság fogalmát a használati utasítás teljesíti, mint annak gyakorlati megvalósulási formája? És ha igen egy használati utasítás mennyire biztosítja az átláthatóságot? Hiszen képzeljük el, hogy egy hozzáértő szakértők által elkészített majd laikusok számára átadott dokumentum mennyire lehet képes megvalósítani a rendelet által is kiemelt egyértelmű tájékoztatást? Továbbá, az AI Act gyakorlati végrehajtása és az ex-ante

jogvédelmi elemzések hatékonysága még tisztázásra szorul. Mindazonáltal a rendelet számos további pozitív iránymutatást tartalmaz a mesterséges intelligenciával kapcsolatos általános ismeretek bővítésére, mint például az MI jártasság,⁶⁸ a gyakorlati kódexek támogatása,⁶⁹ MI hivatal tevékenysége.⁷⁰ Ezeknek a megfelelő alkalmazásával, valamint az EDPD irányelveivel és a bevált gyakorlatok integrálásával lehetőség nyílik az eltérések hatékony áthidalására. Ennek érdekében a továbbiakban javaslatokat fogalmazok meg arra vonatkozóan, hogyan lehetne a helyzetet hatékonyan javítani.

Az első és talán a legfontosabb az átláthatóság kérdésének feloldása egy iránymutatással. Ez a legjelentősebb hiszen a korábbiakban elmondottak szerint a MI fejlesztés és alkalmazás minden mozzanatának, illetve az esetleges alkalmazók és befektetők technológiához való hozzáállásának szempontjából meghatározó az átláthatóság. A második javaslatom egy kiegészítő szabályozás keretében több konkrét jogérvényesítési mechanizmus kialakítása. Ez azért szükséges, mert az érintetteknek, miután átlátják a rendszert és annak működésében esetlegesen hibát észlelnek, olyan egységes, a MI sajátosságait figyelembe vevő eszközökre van szükségük, amelyek lehetővé teszik számukra a problémák megfelelő módon történő orvoslását. A harmadik javaslatom az, hogy az adatvédelmi hatásvizsgálatok és az alapvető jogi hatásvizsgálatok közötti kapcsolódási pontokat tisztázzák, valamint a két vizsgálati típus közötti eredmények újra hasznosítását tegyék egyszerűbbé és egységesebbé. Ez azért is kulcsfontosságú, mert ezek a hatásvizsgálatok nemcsak az érintettek jogainak védelmét szolgálják, hanem részben választ is adhatnak arra a releváns kritikára, miszerint az AI Act túlzott adminisztratív és pénzügyi terhet róhat a MI rendszerek üzemeltetőire. Az egyértelmű szabályok kialakítása elősegítené, hogy a hatásvizsgálati folyamat hatékonyabbá váljon, így a MI fejlesztési láncolat tagjainak a terhei csökkennének.

⁶⁸ AI Act 4. cikk

⁶⁹ AI Act V. fejezet 4. szakasz 56. cikk

⁷⁰ AI Act VII. fejezet 1. szakasz 64. cikk

Irodalomjegyzék:

1. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.), azaz az Általános Adatvédelmi Rendelet (General Data Protection Regulation, GDPR), amely a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmét, valamint az ilyen adatok szabad áramlását szabályozza.
2. Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.), a bűncselekmények megelőzésével, nyomozásával, felderítésével, vádeljárásával és büntetőjogi szankciók végrehajtásával kapcsolatos személyesadat-kezelés szabályozására.
3. Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.), amely a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelésére vonatkozó szabályokat tartalmazza.
4. Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.), az elektronikus hírközlési adatvédelemről (ePrivacy Directive).
5. Busuioc Madalina – Deirdre Curtin – Marco Almada: Reclaiming transparency: contesting the logics of secrecy within the AI Act. *European Law Open* 2.1, Cambridge 2023, 79-105.
6. Claudio Novelli et al.: Taking AI risks seriously: a new assessment model for the AI Act. *AI & Soc.* 39. 2024. 2493-2497.
7. Cisco Systems: Maximizing the value of your data privacy investments – Data Privacy Benchmark Study. Cisco Cybersecurity Series 2019, január.
8. D. Golpayegani - H. J. Pandit - D. 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: *ACM Conference on Fairness, Accountability, and Transparency*, Chicago, 2023. 905–915.
9. Datatilsynet: Artificial intelligence and privacy. Report, January 2018.

10. EDPB: Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). European Data Protection Board, 2021.
11. EDPB: Guidelines on Transparency under Regulation 2016/679.
12. European Commission: Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése. 2020.
13. European Union: Open data and AI: A symbiotic relationship for progress.
14. Forgács Imre: A Big Data, avagy kezdjük el gondolkodni a közigazgatás új feladatairól. In: Fazekas Marianna (szerk.): Gazdaság és közigazgatás: tanulmányok Ficzer Lajos tiszteletére. Budapest, ELTE Eötvös Kiadó, 2015. 123-133.
15. Jonas Schuett: Risk Management in the Artificial Intelligence Act. European Journal of Risk Regulation, 2024. 15(2), 367-385.
16. Kollár Csaba: Kína és a társadalmi kredit rendszere. REAL - az MTA Könyvtárának Repozitóriuma.
17. Mahieu René – Jef Ausloos: Harnessing the collective potential of GDPR access rights: towards an ecology of transparency. Internet Policy Review 3.4, Berlin, 2020.
18. Michael Veale – Lilian Edwards: Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. In: Sophie Stalla-Bourdillon: Computer Law & Security Review. 34(2), Amsterdam, Elsevier, 2018. 398-404.
19. Péterfalvi Attila – Révész Balázs – Buzás Péter: Magyarázat a GDPR-ról. Wolters Kluwer Kft., Budapest, 2018.
20. Rákos Dóra: A személyes adatok védelme az új európai adatvédelmi rendelet (GDPR) tükrében. Opuscula Iuvenum Excellentissima 2019/2. szám, 32-35.

21. Robert Walters - Marko Novak: Cyber Security, Artificial Intelligence, Data Protection & the Law. Springer Nature Singapore, 2021.
22. Stuart Russel – Peter Norvig: Artificial Intelligence: A Modern Approach. New Jersey, Pearson, 2016.
23. Szűts Zoltán és Yoo Jinil: Big Data, az információs társadalom új paradigmája. Információs Társadalom 16(1), 2016. 8-28.
24. The European Commission's High-Level Expert Group On Artificial Intelligence: A Definition Of AI: Main Capabilities And Scientific Disciplines. European Commission, 2018.
25. Tytti Rintamäki et al.: High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications. Exeter, European Journal of Law and Technology, 2023.
26. Üveges István: A feketedoboz jelensége és következményei a mesterséges intelligencia alapú technológiákban. Wolters Kluwer, 2024.
27. Varošanec Ida: On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI. International Review of Law, Computers & Technology, Taylor & Francis, London, 2022.