AZ ADATVÉDELMI TISZTVISELŐ POZÍCIÓJA ÉS SZEREPE A MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ RENDELET KOCKÁZATI RENDSZERÉBEN

dr. Török Tamás Sándor LL.M.
Doktorandusz, Pécsi Tudományegyetem Állam-és Jogtudományi Doktori Iskola
A szerző elérhetősége: tamas.drtorok@gmail.com

DOI: 10.47272/KIKPhD.2024.3.2

ÖSSZEFOGLALÓ

A Mesterséges Intelligencia Rendelettel (AIA) az Európai Unió egy újabb mérföldkőhöz érkezett el a technológiai jogi szabályozások terén. Hasonlóan az általános adatvédelmi rendelethez (GDPR), jelen esetben is a jogalkotás központi motívumaként jelenik meg a kockázatalapú megközelítés, ugyanakkor nem csak emiatt érdemes összevetni a két szabályozási rezsimet.
A személyes adatok védelme a Mesterséges Intelligencia Rendeletben is hangsúlyosan jelenik meg, ugyanakkor a GDPR szabályozásától eltérő mechanizmusok kerültek meghatározásra.
Az adatvédelmi tisztviselő a GDPR megfelelés egyik sarokköve, a személyes adatok védelmének egyik garanciális jogintézménye, amelyhez hasonló szerepkört a AIA nem hívott életre, ellenben az abban foglalt rendelkezések jelentős kihatással vannak rá. Jelen tanulmány az adatvédelmi tisztviselőnek a Mesterséges Intelligencia Rendelettel összefüggésben felmerülő feladatait és szerepét kívánja meg bemutatni.

KULCSSZAVAK
Adatvédelem, mesterséges intelligencia, adatvédelmi tisztviselő, kockázat alapú szabályozás

I. Bevezetés

2024. augusztus 1-jén hatályba lépett az Európai Parlament és a Tanács mesterséges intelligenciáról szóló 2024/1689 számú rendelete (továbbiakban: AIA),[1] amelyet aligha túlzás az elmúlt évek egyik legjelentősebb jogalkotási termékének nevezni.[2]

Az Európai Bizottság már 2018. április 25. napján kiadott közleményében úgy fogalmazott, hogy „*Ahogy korábban a gőzgép és a villamos energia, a mesterséges intelligencia is átalakítja világunkat, társadalmunkat és az ipart*”.[3] A történelmi párhuzam

[1] Az Európai Parlament és a Tanács (EU) 2024/1689 Rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról

[2] Burlacu, Fiorentina - Ghioaldă Lută, Gratiela Doina: The Crucial Importance Of The European Union Ai Act As The World's First Regulation On Artificial Intelligence. *Journal of Information Systems & Operations Management 17*(2), 2023. 59-63. o.

[3] A Bizottság Közleménye – A közös európai adattér kialakítása felé (COM(2018) 237 final)

aligha túlzó. Maga a közlemény már 2018-ban kitér a gazdasági lehetőségek értékalapú kiaknázásának igényére, amely magába foglalja a társadalmi szempontok és az egyéni jogok védelmének garantálását is. Ez utóbbiak közül kiemelt jelentőséggel bír a magánélethez való jog biztosíthatósága a személyes adatok védelmén keresztül.

Az AIA hatásai, értelmezése, tagálami jogalkalmazásra gyakorolt hatásai fokozatosan fognak testet ölteni, kérdések és megoldandó problémafelvetések sorát indikálva. Jelen tanulmányban az új rendelet és egy „régebbi" jogintézménynek kapcsolódási pontjait kívánom elemezni, elsődlegesen a már meglévő joggyakorlat és az AIA normaszövege alapján.

A tanulmány keretei ugyanakkor nem teszik lehetővé egy átfogó vizsgálat lefolytatását, éppen ezért e körben elsődlegesen az AIA által meghatározott MI-rendszerek kockázati megítélésében való lehetséges és potenciális adatvédelmi tisztviselői (továbbiakban: tisztviselő vagy DPO) feladatellátást kívánom elemezni, keresve a privacy by design ebbéli lehetséges értelmezését az új jogi keretrendszerben. Ugyanakkor figyelemmel az AIA kockázati rendszerére és az ahhoz fűződő kötelezettségekre, az elemzés a tiltott, illetve a magas kockázatú MI-rendszerek esetében fellépő tisztviselői szerepkör meghatározását tűzi ki elsődleges célként, mint ahol a legkritikusabb a védelmi funkciók meglétének kérdése.

A kockázat alapú megközelítés, amellyel a jogalkotó fordult az új technológiához, nem előzmény nélküli.[4]

Az AIA (26) preambulumbekezdésében a jogalkotó az alábbi indoklást fűzi a kockázatalapú megközelítés alkalmazásához: „*Az MI-rendszerekre vonatkozó, kötelező erejű szabályok arányos és hatékony rendszerének bevezetése érdekében egyértelműen meghatározott, kockázatalapú megközelítést kell alkalmazni. E megközelítés keretében az ilyen szabályok típusát és tartalmát hozzá kell igazítani az MI-rendszerek által keltett kockázatok intenzitásához és nagyságrendjéhez".*[5]

Az általános adatvédelmi rendelet (továbbiakban: GDPR) (74) preambulumbekezdése hasonló megközelítésről tesz tanúbizonyságot: „*Az adatkezelőt kötelezni kell különösen arra, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek e rendeletnek megfelelnek, és az alkalmazott intézkedések hatékonysága is az e rendelet által előírt szintű. Ezeket az intézkedéseket az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni".* [6]

[4] Ebers, Martin: Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act. *European Journal of Risk Regulation*, 2024. 1-20. o. https://doi.org/10.1017/err.2024.78

[5] AIA (26) premabulumbekezdés

[6] GPDR (74) preambulumbekezdés

Hasonló logika érhető tetten a digitális szolgáltatásokról szóló rendelet (DSA) esetében is,[7] nem véletlenül. A kockázatalapú megközelítés a jogalkotásban a környezetvédelmi, egészségügyi, élelmiszeripari, pénzpiaci, bank és biztosítási szektor, vagy éppen a munkavédelmi szabályozás vonatkozásában figyelhetünk meg, azonban az utóbbi években mind szélesebb szabályozási tárgykörben nyer alkalmazást. A jogalkotás során a kockázat, mint logikai origó egyre dominánsabban jelenik meg a digitális piacok és a digitális társadalom tárgykörét érintő szabályozásában is.[8]

A „kockázat-társadalom" (risk society) fogalmát Ulrich Beck és Anthony Giddens nevéhez köthetjük,[9] ami az emberi döntéseknek a globális kockázatokat generáló aspektusára utal. Így válik értelmezhetővé, hogy a technológiai és politikai környezetünket alapjaiban befolyásoló modern digitális kockázatok azonosítása és kezelése a jogalkotók és a kormányok számára prioritássá vált.[10]

A jog, mint eszköz a felmerülő, technológiai kockázatok kezelése érdekében annyiban és úgy reagál, amennyiben az szükséges a megfelelő egyensúly elérése érdekében. E tárgykörben a kockázat egy adott technológia alkalmazása által megvalósított negatív következmény bekövetkezésének esélyét és nagyságát a bekövetkezés valószínűségének függvényében jelenti.[11]

A szempontrendszer ilyen módosulása célként jelöli meg a túlszabályozás elkerülését, ezzel pedig a jogalanyok megfeleléssel kapcsolatos költségeinek csökkentését, egy hatékonyabb, átláthatóbb és tisztességes magatartást előmozdításának érdekében. A jogalkotás e tekintetben a veszélyekkel arányos megközelítésre helyezi a jogalkalmazók kötelezettségének fő fókuszát, rugalmasságot és nagyobb felhatalmazást engedve a konkrét élethelyzetek megfelelő kezelésének céljából.[12]

II. Az adatvédelmi szabályozás keretei

1. Az elszámoltathatóság alapelve és a kockázat alapú megközelítés

A kockázat alapú megközelítés azt az ésszerűen elvárható előrelátást várja el az érintett szervezetektől, hogy a tevékenységük, vagy jelen esetben az új technológiák

[7] Hohmann, Balázs: A Digital Services Act és a Digital Markets Act termékekreés digitális szolgáltatásokra irányuló fogyasztói jogviszonyokat érintő rendelkezései. *In Medias Res 12*(2), 2023. 70. o. https://doi.org/10.59851/imr.12.2.4

[8] Efroni, Zohar: *The Digital Services Act: risk-based regulation of online platforms*. Internet Policy Review, 2021. https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606 (2024.12.31.)

[9] Beck, Ulrich: *Risk society -Towards a new modernity*. München, University of Munich, 1992. 9-22. o.

[10] Efroni, 2021, i.m.

[11] Mezei Kitti – Träger Anikó: Kockázatok és reziliencia az online platformok és a mesterséges intelligencia európai uniós szabályozásában, *MTA Law Working Papers* 2024/1. 7. o.

[12] Mezei– Träger, 2024, i.m. 47. oldal

használata előtt felmérjék azok alkalmazásának lehetséges hatásait és megtegyék a szükséges intézkedéseket az esetleges kockázatok minimalizálása érdekében. Megfogalmazható ez az elvárás úgy is, mint az adott szervezet preventív compliance programja, vagyis a jogszabályi, de tágabb értelemben a társadalmi és etikai elvárásoknak megfelelő működés kialakításának kötelezettsége.

A kockázat alapú megközelítést a GDPR zsinórmértékként alkalmazza a privacy jellegű kockázatok értékelésének és kezelésének vonatkozásában, ugyanis amíg a személyes adatok kezelése negatív hatást képes kiváltani az érintettek jogaira és szabadságaira, addig a védelmi intézkedések meghozatala elvárt és indokolt.[13]

Amennyiben tehát a kockázatkezelést elfogadjuk preventív compliance tevékenységnek, úgy a GDPR által alapelvi szinten megfogalmazott elszámoltathatóság elvét is érdemes ebben a kontextusban értelmezni és vizsgálni.[14]

Az elszámoltathatóság elve[15] alapozza meg azt az adatkezelési keretrendszert, amelyben az adatkezelő az adatkezelés teljes életciklusára vetítetten, a tervezéstől a megvalósulásig folyamatszinten adminisztrálja tevékenységét, ezzel biztosítva a GDPR rendelkezéseinek való megfelelést a külvilág felé.[16] Az elszámoltathatóság transzparenciát eredményez,[17] amely az elvárásoknak megfelelő tájékoztatók, szabályzatok, nyilvántartások, eljárásrendek elkészítése és megismerhetősége révén átláthatóvá és nyomon követhetővé teszi az adott adatkezeléseket mind az érintettek, mind pedig a felügyeleti hatóságok irányába. [18]

A GDPR előírásainak való megfelelést önmagában nem fogja eredményezni csak a jogszabályok által expressis verbis megfogalmazott elvárások betartása, ezen túlmenően, az érintettek várakozásaira is figyelemmel kell lenni. Ezt a meggondolást támaszatja alá a jogos érdek vonatkozásában megfogalmazott, a (47) preambulumbekezdés „számíthat-e észszerűen" fordulata, amely a megfelelés egyik záróköveként jelöli meg az érintettek jogilag akceptálható előfeltevéseihez való igazodást.[19]

Ebből következik, hogy valamennyi adatkezelési művelet előtt fel kell mérni és értékelni kell a lehetséges kockázatokat úgy, hogy azok a strict jogszabályi előírásokon túl vegyék figyelembe az adott érintetti csoport azon jellemzőit is,

[13] Szabó Endre Győző: Az Adatvédelmi tisztviselőről, a GDPR szabályainak elemzése, *Infokommunikáció és Jog*, 2018/1. 3. o.

[14] De Hert, Paul – Lazcoz, Guillermo: When GDPR-principles blind each other: accountability, not transparency, at the heart of algorithmic governance. *European Data Protection Law Review 8*(1), 2022. 31. o. https://doi.org/10.21552/edpl/2022/1/7

[15] GDPR 5. cikk (2) bekezdés

[16] Péterfalvi Attila – Révész Balázs – Buzás Péter (Szerk.): *Magyarázat a GDPR-ról*, Budapest, Wolters Kluwer Hungary, 2021. 141. o.

[17] Hohmann Balázs: Interpretation the Concept of Transparency in the Strategic and Legislative Documents of Major Intergovernmental Organizations. *Közigazgatási és Infokommunikációs Jogi Phd Tanulmányok* 2(1), 2021. 48-68. o. https://doi.org/10.47272/KIKPhD.2021.1.4

[18] Péterfalvi – Révész – Buzás, 2021, i.m. 142. o.

[19] Szabó, 2018, i.m. 4. o.

amelyek esetleg befolyásolhatják az adatkezeléssel szemben támasztott elvárásaikat úgy, hogy a döntés mechanizmusa és eredménye transzparens módon dokumentált és adott esetben egy hatósági eljárásban (bizonyos esetben érintetti megkeresés esetén is) bemutathatóvá váljon.[20]

Az elszámoltathatóság elve egyszersmind a kockázatkezelés megfelelősségének ellenőrizhetőségét, a kockázatkezelési mechanizmusok áttekinthetőségét is szolgálja.

A GDPR számos rendelkezését tartalmaz a „megfelelősségi" intézkedésekkel és azok igazolhatóságával összefüggésben, mint például az adatkezelési tevékenységek belső nyilvántartásának (GDPR 30. cikk), adatvédelmi hatásvizsgálat (GDPR 37. cikk) elvégzésének, adatvédelmi incidensek során elvárt eljárásoknak (GDPR 34. cikk) és az adatvédelmi tisztviselő kijelölésének (GDPR 37. cikk) szabályai.[21]

Jelen tanulmány fókuszában ez utóbbi, vagyis az adatvédelmi tisztviselő jogintézménye áll, ami egyszerre része és támogatója az elszámoltathatóság érvényesülésének, következésképp a GDPR-ban meghatározott kockázatkezelés hatékonyságának záloga is.

2. Az adatvédelmi tisztviselő helye és szerepe a kockázatkezelésben

Az adatvédelmi tisztviselő kijelölésének, jogállásának és feladatainak szabályait a GDPR 4. szakasza tartalmazza, ugyanakkor a nevezett szervezeten belüli funkció már jóval az általános adatvédelmi rendelet előtt is létezett. Az adatvédelmi tisztviselő az Egyesült Államok nagyvállalatai működésének és szervezeti kultúrájának szerves részét képezte. A „privacy officer", vagy a „chief privacy officer" olyan munkatársat jelölt, akinek a magánélet védelmi körébe tartozó személyes adatok kezelésének jogszerű és etikus kezelése, az ehhez kapcsolódó belső folyamatok kialakítása és támogatása volt a feladata.[22] Az európai jogrendszerbe az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve (továbbiakban: irányelv) ültette át az adatvédelmi tisztviselő jogintézményét, ugyanakkor a kijelölés az adatkezelők esetében nem vált kötelezettséggé, csupán olyan opcióvá, amelyhez bizonyos előnyöket társított a

[20] Hohmann Balázs: *A mesterséges intelligencia közigazgatási hatósági eljárásban való alkalmazhatósága a tisztességes eljáráshoz való jog tükrében*. In: Török Bernát – Ződi, Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai – Tanulmányok a mesterséges intelligencia és a jog határterületeiről*. Budapest, Ludovika Egyetemi Kiadó, 2021. 403-422. o.
Szőke Gergely László: *Big Data and Algorithms in the Public Sector and Their Impact on the Transparency of Decision-Making*. In: Hansen, Hendrik, et al. (Szerk.): *Central and Eastern European eDem and eGov Days 2018 : Conference proceedings*. Wien, Facultas Verlag, 2018. 301-303. https://doi.org/10.24989/ocg.v331.25
[21] Péterfalvi – Révész – Buzás, 2021, i.m. 141. o.
[22] Justine Brown*: Rise of the Chief Privacy Officer*. Government Technology, 2014. https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html (2024.12.31.)

jogszabály, azonban kötelezővé nem tette azt még a nagy kockázatú adatkezeléseket végző szervek vagy szervezetek részére sem.

A 29. cikk szerinti munkacsoport (továbbiakban: Munkacsoport) WP 243 rev.01 számú iránymutatása részletesen foglalkozott az adatvédelmi tisztviselő feladatainak és hatáskörének kérdésével, amely alapelvek napjaink joggyakorlatát is alapjaiban határozzák meg.

A Munkacsoport az elszámoltathatóság alapköveként hivatkozott az adatvédelmi tisztviselőre, mely funkció segíthet a jogszabályi megfelelésben, illetve feladatköréből fakadóan a bizalom, így pedig a végsősoron a vállalkozások versenyelőnyét is képes előmozdítani.[23]

Az adatvédelmi tisztviselő az általános adatvédelmi rendelet komplex védelmi rendszerének egyik alapeleme, az elszámoltathatóság és így a rendeletben foglalt előírásoknak való megfelelés központi garanciája. A rendelet (77) preambulumbekezdése szerint „*A megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához - különösen ami az adatkezeléssel kapcsolatos kockázat beazonosítását, valamint a kockázat forrásának, jellegének, valószínűségének és súlyosságának a felmérését illeti -, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak az azonosításához útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások*". Mindezen státuszát az adatvédelmi tisztviselőnek a (49) preambulumbekezdésben foglaltak töltik fel valódi tartalommal, mely szerint „*az adatvédelmi tisztviselőt, függetlenül attól, hogy az adatkezelő alkalmazottja-e vagy sem, olyan hatáskörrel kell felruházni, hogy feladatát teljesen függetlenül gyakorolhassa*."

Az adatvédelmi tisztviselő megkülönböztetett helye és szerepe az adatvédelmi jogszabályok érvényesülését szolgáló jogintézmények között aligha megkérdőjelezhető. A GDPR rendelkezéseivel összhangban álló adatkezelői – és bizonyos esetekben adatfeldolgozói- magatartást függetlenül, tanácsadással előmozdító funkció átfogó felkészültséget igényel.

A szerepkör komplexitására és súlyára tekintettel az Infotv. korábban meghatározott végzettség megléte esetében tette lehetővé a belső adatvédelmi felelősi pozíció betöltését. Ennek értelmében „*jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel*",[24] lehetett csak valaki belső adatvédelmi felelős. A GDPR ettől eltérően nem végzettség orientáltan, hanem kompetencia alapon határozza meg a kijelölés feltételeit. Így az adatvédelmi tisztviselőnek mindenekelőtt

[23] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról

[24] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24. § (1) bekezdés 2018. július 25-ig hatályos szövege.

megfelelő szakmai rátermettséggel, szakmai ismeretekkel és a feladatellátást lehetővé tevő képességekkel kell rendelkeznie.[25]

A GDPR által alkalmazott követelményrendszer egyszerre tekinthető megengedőbbnek és szigorúbbnak, mint a korábbi magyar szabályozás. Megengedőbb, hiszen a jogalkotó által korábban megjelölt végzettség hiányában is lehetőséget biztosít adatvédelmi tisztviselői feladatok ellátására, ugyanakkor az átfogó és komplex ismeretek kritériumrendszere a korábban statikus elvárásokat dinamikussá tette. Hiszen a rendeletben foglalt „*az adatvédelmi jog és gyakorlat szakértői szintű ismerete*" kitétel permanens elvárásként azonosítható, amelynek az adatvédelmi tisztviselők csak folyamatos képzés és ismereteik naprakészen tartása mellett tudnak megfelelni!

Különösen igaz ez a (97) preambulumbekezdés ismeretében, amely értelmében az adott tisztviselő *szakértelmének megfelelő szintjét*, mint elvárást mindig az adatkezelő vagy adatfeldolgozó konkrét tevékenységének, továbbá a személyes adatok védelmének elvárt szintje alapján lehet meghatározni.[26]

Mint az látni fogjuk, az adatvédelmi tisztviselő naprakész szakmai ismereteinek rendeletből fakadó követelményének különös jelentősége lesz az AIA megfelelés vonatkozásában is, hiszen a mesterséges intelligencia rendszerek személyes adatokkal való kapcsolata során elengedhetetlen a tisztviselői kontrollfunkciók hatékony működése.

2.1. Adatvédelmi tisztviselő kijelölése

A GDPR egyértelmű rendelkezéseket tartalmaz arra nézve, hogy mely adatkezelőknek és adatfeldolgozóknak kötelező adatvédelmi tisztviselőt kineveznie. A kijelölési kötelezettség elsődlegesen a szervezetek tevékenységével áll összefüggésben. Kötelező a kijelölés a közhatalmi vagy egyéb, közfeladatot ellátó szervek esetében, továbbá azon adatkezelőknél és adatfeldolgozóknál, ahol a főtevékenység végzése olyan adatkezelést eredményez, amely jelentős hatást képes gyakorolni az érintettek magánéletére.[27]

Az AIA összefüggésében a fő kérdés az, hogy módosulhat-e a jelenleg kialakult, adatvédelmi tisztviselői kijelölésre irányadó joggyakorlat akkor, ha az adott adatkezelő vagy adatfeldolgozó bizonyos MI-rendszerek alkalmazását kezdi meg?

Következésképp jelen körben semmiképp sem a közhatalmi szervek, illetve közfeladatot ellátó szervek kötelező kijelölés eseteit, hanem a GDPR 37. cikk (1) bekezdés b)[28] pontjában rögzített feltételek vizsgálatát kell, hogy érintse a vizsgálat.

[25] Péterfalvi – Révész – Buzás, 2021, i.m. 418. o.
[26] U.o. 419. o.
[27] U.o. 413. o.
[28] Hivatkozott szakasz úgy fogalmaz, hogy az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé.

Az adatkezelő, adatfeldolgozó főtevékenységének, illetve az érintettek rendszeres és szisztematikus, nagymértékű megfigyelésének megítélésével vonatkozó állásfoglalásában az adatvédelmi munkacsoport is részletesen foglalkozott.[29] Főtevékenység alatt a munkacsoport az adatkezelő, adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket érti azzal, hogy a „fő tevékenység" definíciójának ki kell terjednie valamennyi olyan aspektusra is, amely az adott szerv (legyen az adatfeldolgozó vagy adatkezelő) tevékenységének elválaszthatatlan részét képezi.[30]

Ugyancsak értelmezésre szorul a „nagy mértékű" kitétel. Azt a Munkacsoport is leszögezte, hogy egzakt határértékeket nincs lehetőség megállapítani, azonban vannak olyan szempontok, amiket a mérlegelés során alapul kell venni:

- Az érintettek száma, vagy konkrét, vagy népességarányos meghatározással,
- Az adatok mennyisége és/vagy a kezelés alá vont adatok köre,
- Az adatkezelési tevékenység permanenciája,
- Az adatkezelési földrajzi kiterjedtsége.

A Munkacsoport kitért az érintettek rendszeres és szisztematikus megfigyelésének elemzésére is. Az általános adatvédelmi rendelet e körben sem alkalmaz konkrét definíciót, csupán a (24) preambulumbekezdés utal az érintettek interneten való nyomon követesére és a profilalkotásra, ugyanakkor természetesen aligha értelmezhető ilyen szűkítően a fogalompár. Az iránymutatás a rendszeresség esetében az időben való szabályszerűen visszatérő jelleget hangsúlyozza, míg a „szisztematikus" kifejezést a módszeresség és megszervezettség jegyeinek meglétével tartja igazolhatónak. Érdemes megjegyezni, hogy a Munkacsoport iránymutatásában az érintettek rendszeres és szisztematikus megfigyelésének példájaként már hivatkozza az intelligens mérőberendezések, intelligens gépjárművek vagy éppen a lakásautomatizálás technológiáját[31], amelyek értelmezhetőek akár a mesterséges intelligencia előszobájaként is.

Az adatvédelmi tisztviselő kijelölésének kötelezettsége tehát az adatkezelő és adatfeldolgozó fő tevékenységének függvényében állapítható meg, amely fogalom viszont tágan értelmezendő, magába foglalva így nem csak az adott szervezet fő céljait, hanem az azokhoz szükségszerűen kapcsolódó tevékenységeket is. Könnyű belátni, hogy olyan esetekben, mikor az adatkezelő vagy adatfeldolgozó fő tevékenységének támogatása érdekében MI-rendszert alkalmaz, úgy fokozott figyelemmel szükséges ellenőrizni az adatvédelmi tisztviselő kijelölésére irányadó szabályokat, ugyanis az egyes MI-rendszerek a cél és felhasznált adatok függvényében akár olyan szervezeteknél is indikálhatják a DPO kijelölésének

[29] Article 29 Data Protection Working Party: *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01) (a továbbiakban WP 243 rev.01.) 9. o.
[30] U.o.
[31] WP 243 rev.01., i.m. 9-10. o.

szükségességét, amelyeknél ilyen rendszerek alkalmazása nélkül egyébként erre nem lenne kötelezettség.

2.2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő az adatvédelmi jogszabályokról és azok helyes alkalmazásáról tanácsot ad adatkezelőnek, ideértve adatkezelő munkavállalóit is. A tanácsadás mellett a megfelelés ellenőrzése képezi a legfontosabb kötelezettséget, ugyanis mind a jogszabályok, mind pedig az adatkezelőre, adatfeldolgozóra irányadó belső szabályok érvényesülését felügyeli a DPO. [32]

A megfelelés ellenőrzése magába foglalja többek között az információk beszerzését, az adatkezelési tevékenységek elemzését épp úgy, mint a tájékoztatások és adott esetben ajánlások kiadásának lehetőségét is. [33] A beépített adatvédelem elvéből következik, hogy valamennyi, a személyes adatok kezelését magába foglaló művelet és folyamat tervezésének már a legelején, megfelelő időben szükséges bevonni az adatvédelmi tisztviselőt, aki így a tanácsadást és megfelelésellenőrzést már a kockázatok feltérképezésének fázisában is biztosítani tudja.[34]

A tisztviselőnek megkülönböztetett szerepe és feladata van az adatvédelmi hatásvizsgálatok, illetve a felügyeleti hatóságokkal való kapcsolattartás biztosításának tekintetében. [35]

Az általános adatvédelmi rendelet kockázatközpontú logikája az adatvédelmi tisztviselő feladatainak meghatározásában is megjelenik, ugyanis a 39. cikk (2) bekezdése alapján a DPO feladatait „*az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi*". A Munkacsoport egyfajta „józan ész" szerinti zsinórmértékként hivatkozik a bekezdésben foglaltakra, mint ami a tisztviselő feladat-priorizálását hivatott előmozdítani, lehetővé téve a kockázatokra tekintettel a különböző adatkezelési művelet közötti figyelem- és erőforrásmegosztást. [36]

A tanácsadás és ellenőrzés tehát az adatvédelmi tisztviselői feladatok alap attribútumai. Ezek mentén értelmezhető az adatkezelői, adatfeldolgozói szervezetrendszerben elfoglalt helye a pozíciónak, ami a megfelelést és annak bizonyíthatóságát hivatott garantálni. Ezen szerepkör a beépített adatvédelem elvének érvényesülésével megteremti annak lehetőségét, hogy valamennyi, a személyes adatokat érintő folyamat felett emberi kontroll érvényesüljön, amely kitétel különösen az AIA függvényében nyer majd többlet jelentést.

[32] Szabó, 2018, i.m. 8. o.
[33] WP 243 rev.01., i.m. 20. o.
[34] Szabó E. in. 2018, i.m. 8. o.
[35] WP 243 rev.01., i.m. 20. o.
[36] WP 243 rev.01., i.m. 21. o.

III. A Mesterséges Intelligencia Rendelet: kockázatalapúság és a magánélet védelmének egyes kérdései

1. AIA és a személyes adatok védelme

Az AIA maga is számos rendelkezést tartalmaz a természetes személyek személyes adatainak védelmével összefüggésben. Érdemes ezen a ponton utalni az AIA (10) preambulumbekezdésére, amely értelmében *az MI-rendszerek forgalomba hozatalára, üzembe helyezésére és használatára vonatkozó, e rendelettel megállapított harmonizált szabályoknak meg kell könnyíteniük, hogy az érintetteket a személyes adatok és egyéb alapvető jogok védelmére vonatkozó uniós jog értelmében megillető jogok és egyéb jogorvoslatok ténylegesen érvényesüljenek, illetve lehetővé kell tenniük az említett jogok és egyéb jogorvoslatok érintettek általi gyakorlását.*

A személyes adatok fokozott védelmére irányuló kötelezettségek vonatkozásában elégséges csupán megemlíteni az AIA 10. cikk (2) és (5) bekezdésében foglalt, a nagy kockázatú MI-rendszerek által használt tanító-, validálási és a tesztadatkészletek személyes adatokat érintő előírásait, vagy éppen az 50. cikk (3) bekezdését, amely az érzelemfelismerő rendszer vagy a biometrikus kategorizálási rendszer alkalmazásával összefüggésben utal kifejezetten az ilyen adatok védelmére.

Látható, hogy az AIA hangsúlyosan kezeli a személyes adatok védelmének kérdését, amit alátámaszt többek között a hivatkozott preambulumbekezdés megfogalmazása is, ahogy a jogalkotó azt megkülönböztető jelleggel, külön nevesítve emelte ki a többi alapjog közül. Az MI-rendszerek, különösen a profilalkotás és az automatizált döntéshozatal területén valójában szignifikáns kockázatokat hordoznak a természetes személyek személyes adatainak védelme terén, így indokolt és célszerű is fokozott figyelmet fordítani a két szabályozási rezsim egymással való kölcsönhatására.

2. Az AIA kockázatrendszerének kontextusa

Látható, hogy mind a GDPR, mind az AIA – hasonlóan más, technológiai tárgyú szabályozásokhoz- esetében kockázat alapú megközelítést érvényesített a jogalkotó. Az AIA alkalmazásában is azt a bevett gyakorlatot követi a jogalkotó, miszerint a kockázat az nem más, mint a kár bekövetkezési valószínűségének és az említett kár súlyosságának kombinációja.[37] A kockázat, mint központi fogalom egyszersmind annak beismerése is, hogy a teljeskörű biztonság elérése nem reális. Ha pedig ezt elfogadjuk, akkor célként csak a kockázatok egy meghatározott szintre csökkentése jelölhető meg, olyan szintre, ami az adott közösség, társadalom számára még elfogadható.[38]

[37] AIA 3. cikk 2. pont

[38] Tóth András: Az Európai Unió Mesterséges Intelligencia Törvényéről. *Gazdaság és Jog*, 2024/5-6. 3-11. o.

Az AIA a kockázatalapú megközelítés jegyében az MI- rendszerek esetében az általuk hordozott és jelentett kockázat alapján négy csoportot különböztet meg. Így beszélhetünk elfogadhatatlan kockázattal, nagy vagy magas kockázattal, korlátozott kockázattal, illetve a minimális kockázattal működő MI-rendszerről. A jelzett kategóriákon kívül az AIA külön rendelkezéseket tartalmaz az úgynevezett általános célú MI- rendszerek (GPAI) tekintetében. [39] A kockázat alapú besorolás esszenciális jelentőségű, ugyanis a jogalkotó az eltérő csoportokhoz eltérő követelményeket, jogalkalmazói magatartásokat rendel. Ezen megközelítésben manifesztálódik az az európai uniós jogalkotásban megfigyelhető bináris szemlélet, ami az alapvető jogok védelmét hivatott előmozdítani, nevezetesen, hogy minden alapvető jognak van egy „lényege", amit védeni kell, ugyanakkor ezen túlmenően a jogvédelem az optimalizálásra törekszik. Az alapvető jogokat tehát a lehető legnagyobb mértékben kell védelmezni, azokat csak az arányosság elvét figyelembe véve lehet korlátozni.[40]

Az AIA által megjelölt MI-rendszerkategóriák tehát egyfajta *alapjogi lépcsőt* is megtestesítenek. A társadalmi érdekekre és egyéni jogokra különböző kockázatot jelentő MI-rendszerekkel szemben más védelmi szintet vár el a jogalkotó, ami egyszersmind azt is jelenti, hogy a jogalkalmazóknak erre figyelemmel kell saját belső megfelelési keretrendszerüket felkészíteni és átalakítani. Az MI-rendszerek bevezetését és használatát megelőzően tehát nem csak az expressis verbis megfogalmazott regulációs elvárásoknak, hanem a mindenkor fennálló társadalmi és egyéni jogvédelmi igényeknek is meg kell tudni felelnie a jogalkalmazóknak.

Ezen a ponton érdemes részleteiben is megvizsgálni az AIA által megjelölt MI-rendszerek kockázati kategóriáit, kiemelt figyelemmel a személyes adatok megjelenésére.

Az AIA 5. cikk taxatív felsorolásban határozza meg, hogy milyen MI-rendszerek használata tilalmazott. Így

- tudatalatti, manipulatív technikák alkalmazása, amelyek célja, hogy egy személy viselkedését befolyásolja, vagy döntési képességét lerontsa,
- adott személy életkor, fogyatékosság, társadalmi vagy gazdasági deprimáltságból eredő sebezhetőségét célzottan kihasználó alkalmazás,
- egyének vagy csoportok viselkedés vagy személyes tulajdonságaik, személyiségi jegyeik alapján történő értékelése, osztályzása,
- egyes személyek kockázatértékelése a bűncselekmény elkövetésére való esély meghatározása érdekében,
- arcfelismerőadatbázis létrehozása vagy bővítése interneten elérhető, vagy zártláncú televízió-felvételek nem célzott lekérdezésével,

[39] U.o.

[40] Almada, Marco – Petit, Nicolas: The EU AI Act: Between Product Safety and Fundamental Rights. *Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59*.

- természetes személyek érzelmeiből következtetni képes MI-rendszer alkalmazása munkahelyi vagy oktatási környezetben,
- biometrikus kategorizálási rendszerek alkalmazása, amelyek célja a természetes személyek faji, politikai, szexuális életük, vallási vagy világnézeti meggyőződésük, szakszervezeti tagságuk kikövetkeztetése megvalósulhasson,
- „valós idejű" távoli biometrikus azonosító rendszerek használata nyilvános helyen, bűnüldözési célból, amely kitétel alól ugyanakkor a rendelet biztosít kivételt.

A tiltott Mi-gyakorlatok tehát azokat a célokat és körülményeket jelölik, amelyek mentén az új technológia nem válik alkalmazhatóvá. Ugyanakkor a megjelölt felhasználási tilalmak mindegyikének előfeltétele a személyes adatok[41] kezelése, amelyek nélkül nem volna lehetséges az adott rendszer alkalmazásáról beszélni. Ez alól esetleg az első tilalom, a *tudatalatti, manipulatív technikák* esetében merülhet fel annak lehetősége, hogy nem személyre szabott, hanem bizonyos csoportjellemzők alapján alkalmazott felhasználásra is lehetőség nyílik, azonban ebben az esetben is megvalósul a személyes adatok kezelése annyiban, hogy a befolyásolni kívánt személy meghatározott paraméterei (mint például életkor, lakóhely, iskolai végzettség stb., amelyek szintén személyes adatnak minősülnek) teszik a manipulációs kísérlet „célpontjává".

Érdemes ugyanakkor megjegyezni, hogy lehetséges – különösen a szubliminális technikák esetében- olyan eljárás, ami kifejezett perszonális targetálás nélkül kíván ilyen rendszert alkalmazni, amely esetben személyes adatok nem kerülnek felhasználásra, azonban ezek hatékonysága messze elmarad a személyre szabott alkalmazási lehetőségekkel szemben, így jóval nagyobb valószínűséggel számíthatunk e körben is a személyes adatok potenciális megjelenésére.

A tiltott MI- gyakorlatok egyszersmind a személyes adatokra, így pedig a természetes személyek jogaira és szabadságaira vonatkozó legsúlyosabb kockázatokat jelölik, tehát a rendeletben kifejtett esetek kivételével nincs helye a forgalomba hozatal, üzembe helyezés vagy használat vonatkozásában mérlegelésnek, ha az adott rendszer célja kimeríti a felsorolt kategóriák valamelyikét.

A tiltott MI-gyakorlatokkal összefüggésben az adatvédelmi tisztviselői feladat főszabály szerint a prevencióra korlátozódik, vagyis a GDPR 39. cikk (1) bekezdés b) pontja értelmében ellenőrzi az irányadó jogszabályoknak való megfelelést, és amennyiben elfogadjuk azt, hogy a nevezett tilalmak személyes

[41] A GDPR 4. cikk 1. pontja értelmében „személyes adat": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

adatok felhasználásával kell, hogy együtt járjanak, úgy a megfelelés e körben csak az előzetes észlelést és bevezetést meggátoló tevékenységként értelmezhető.
A gyakorlatban azonban nem feltétlenül lehet ilyen egyértelmű válaszvonalakat húzni. Erre példaként érdemes említeni az AIA 5. cikk (1) bekezdés f)[42] pontjában foglaltakat. Hivatkozott pontban egyértelmű jogalkotói szándék fedezhető fel: az emberi érzelmeket, mint a magánélet (privacy) legbelsőbb, legszemélyesebb magját kívánják oltalomban részesíteni. Mégis kettős feltételrendszer rajzolódik ki. A tilalom maga ugyanis csak a munkahelyi, illetve oktatási intézmények területére korlátozódik, kivéve, ha a használata, üzembe helyezése vagy forgalomba hozatala orvosi vagy biztonsági okokból történik.

A hatályos magyar szabályozás értelmében munkahelyi környezetben a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, amihez a munkáltató technikai eszközt is alkalmazhat.[43] Ugyanakkor a megfelelő tájékoztatás mellett természetesen az ilyen ellenőrzésnek is meg kell felelnie a GDPR 5. cikkében rögzített alapelveknek, így -többek között- a tisztességes adatkezelés elvének is. Ez zárja ki az olyan elektronikus megfigyelőrendszer alkalmazásának lehetőségét, amely alkalmas a munkavállalók és az általuk végzett tevékenység folyamatos, állandó jellegű megfigyelésére.[44]

Munkahelyi környezetben a természetes személyek érzelmeiből következtetést levonó MI-rendszer alkalmazása csak abban az esetben lehet jogszerű, ha annak célja orvosi vagy biztonsági okokra visszavezethető ellenőrzés, vagyis a munkavállalók fizikai, egészségi állapotának megóvását, megőrzését biztosító technológiai környezet kialakítását szolgáló intézkedésnek felel meg. Nehéz volna egy ilyen rendszer jogszerű működtetését elképzelni a GDPR 35. cikk szerinti adatvédelmi hatásvizsgálat lefolytatása nélkül, amelyben – mint az elszámoltathatóság egyik eszköze- az adatvédelmi tisztviselőnek a tanácsát kötelező kikérni.

A tiltott MI-rendszerek kiszűrése, amennyiben azok személyes adatokat is kezelnének, egy olyan feladat, amelybe az adatvédelmi tisztviselő bevonása – a beépített és alapértelmezett adatvédelem kötelezettségének való megfelelés okán is- elkerülhetetlennek mutatkozik. Ez természetesen nem csak az adatkezelő szervezetre, hanem magukra az adatvédelmi tisztviselőkre is többlet kötelezettséget

[42] A természetes személyek érzelmeiből következtetést levonó MI-rendszerek forgalomba hozatala, e konkrét célra történő üzembe helyezése, illetve használata a munkahelyek és az oktatási intézmények területén, kivéve amennyiben az MI-rendszer használata, üzembe helyezése vagy forgalomba hozatala orvosi vagy biztonsági okokból történik.

[43] A munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) 11/A. § (1) bekezdés

[44] NAIH: *Munkahelyi kamerás megfigyelés szabályai és jogszerűsége*. https://naih.hu/files/dr-Horuczi-Szilvia_A-munkahelyi-kameras-megfigyeles-szabalyai_PPT_STARII-zarokonferencia.pdf (2024.12.31.)

telepít, hiszen a GDPR 37. cikk (5) bekezdésében foglalt *szakmai rátermettség*[45] kifejezés magába kell, hogy foglalja azokat az ismereteket is, amelyek az adatvédelmi jogszabályok és joggyakorlat ismeretén túl elengedhetetlenek a teljeskörű feladatellátáshoz.

Ez utóbbi értelmezést támasztja alá az EDBP riportja is, amelyben az Európai Adatvédelmi Testület kifejti azon álláspontját, miszerint az adatvédelem és a magánélet védelmét biztosító jogi környezet gyorsan és dinamikusan változó terület, amiből következik, hogy az adatvédelmi tisztviselőknek nem elégséges pusztán az ehhez kötődő joggyakorlat és jogszabályi környezet naprakész ismerete. A szakmai ismereteknek ki kell terjedniük az európai adatvédelmi irányelvekkel kapcsolatos új irányokra is, kiváltképp az úgynevezett „Big Five" jogszabályokra is (a digitális szolgáltatásokról szóló rendelet, digitális piacokról szóló jogszabály, adatkormányzási rendelet, adatrendelet és a mesterséges intelligencia rendelet).[46]

3. A nagy kockázatú MI-rendszerek

Az AIA a tiltott MI-rendszereket követően rendelkezik az úgynevezett nagy kockázatú MI-rendszerekről.

Egy MI-rendszer nagykockázatúként való besorolása nem csak az ellátott funkciótól függ, hanem attól is, hogy milyen cél érdekében és milyen módon kerül alkalmazásra. [47]

A rendelet két fő kategóriáját különbözteti meg a fejezetben tárgyalt MI-rendszereknek:

a)az MI-rendszereket az AIA III. mellékletben felsorolt területek valamelyikén kívánják használni;[48]

b) az MI-rendszerek az egészségre és a biztonságra nézve károsodás, vagy az alapvető jogokra nézve kedvezőtlen hatás kockázatát jelentik, és az említett kockázat megegyezik a károsodás vagy a kedvezőtlen hatás azon kockázatával, amelyet a III. mellékletben már említett nagy kockázatú MI-rendszerek jelentenek, vagy annál nagyobb.[49]

A biometrikus azonosítás és az érzelemfelismerő rendszerek, amennyiben nem esnek a tiltott MI-rendszerek meghatározási körébe, úgy magas kockázatúnak fognak minősülni.[50] Az ilyen rendszerek forgalomba hozói kötelesek tájékoztatást

[45] GDPR 37. cikk (5) Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni.

[46] EDPB*: Coordinated Enforcement Action Designation and Position of Data Protection Officers* (2023)

[47] Tóth, 2024, i.m. 3-11. o.

[48] AIA 7. cikk (1) bekezdés a) pont

[49] AIA 7. cikk (1) bekezdés b) pont

[50] Barkane, Irena: Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance. *Information Polity 27*(2), 2022. 147-162. o. https://doi.org/10.3233/IP-211524

nyújtani az érintettek részére a rendszer működéséről. A tájékoztatási kötelezettség alól csak abban az esetben lehet mentesülni, ha az alkalmazott rendszert bűncselekmények felderítése, megelőzése és kivizsgálása céljából jogszabály engedélyezi, azonban ekkor is biztosítani kell harmadik felek jogainak és szabadságainak megfelelő védelmét az uniós rendelkezésekkel összhangban.[51]

A kockázat alapú megközelítés megjelenik e körben is, ugyanis az AIA nem tekinti nagy kockázatúnak az adott MI-rendszert, ha annak működése nem jelent jelentős kockázatot a természetes személyek egészségére, biztonságára vagy alapvető jogaikra nézve ideértve természetesen azt is, ha nem történik lényeges befolyásolás a döntéshozatal eredményére.

Ugyanakkor, ha egy III. mellékletben említett MI-rendszer profilalkotást végez, azt minden esetben nagy kockázatú rendszerként kell azonosítani.[52]

Az AIA differenciált megközelítést alkalmaz a kötelezettségek tekintetében attól függően, hogy a magas kockázatú mesterséges intelligencia rendszerek vonatkozásában az egyes szereplők milyen minőségben jelennek meg. Az előírások részletes felsorolása meghaladná a jelen tanulmány rendelkezésére álló lehetőségeket, így ezen a ponton csak utalnék a megfelelésértékelés követelményére, amely – hasonlóan a GDPR által többek között a hatásvizsgálati mechanizmus során támasztottokhoz- nem csupán egy egyszeri, hanem egy folyamatos nyomon követést vár el, a változások jellegéhez mérten pedig felülvizsgálati kötelezettséget is támaszt a rendszerrel összefüggésben.[53]

Fontos harmonizációs rendelkezést tartalmaz az AIA 27. cikke, amely az alapjogi hatásvizsgálat kötelezettségéről rendelkezik. Azon magas kockázatú MI-rendszerek bevezetése előtt, amelyek alkalmazói az AIA 27. cikk (1) bekezdésben foglaltaknak megfelelnek, alapjogi hatásvizsgálatot szükséges elvégezniük, aminek ki kell térnie a rendszer alkalmazásának folyamatleírására, a rendszer használatának gyakoriságára, az érintettek csoportjának meghatározásra, ezen személyi körre irányuló kockázatok bemutatására, a feltárt kockázatok csökkentésére irányuló intézkedésekre- ideértve a belső irányítás és panaszkezelés szabályait is- továbbá az emberi felügyeleti mechanizmus ismertetésére. [54]

Ugyanezen cikk (4) bekezdése rendelkezik arról, hogy amennyiben a GDPR, vagy a bűnügyi adatvédelmi irányelv alapján elkészített adatvédelmi hatásvizsgálat alapján már az alkalmazó megfelelt a fentebb hivatkozott kötelezettségek bármelyikének, úgy az alapvetőjogi hatásvizsgálatnak ki kell egészítenie az említett adatvédelmi hatásvizsgálatot.[55]

[51] Tóth, 2024, i.m. 3-11. o.
[52] AIA 6. cikk (3) bekezdés d) pont
[53] AIA 43. cikk
[54] AIA 27. cikk (1) bekezdés
[55] AIA 27. cikk (4) bekezdés

A GDPR 35. cikk (2) bekezdése értelmében amennyiben az adatkezelőnél van adatvédelmi tisztviselő kinevezve, úgy az adatvédelmi hatásvizsgálat elvégzésekor annak szakmai tanácsát kötelező kikérni.[56]

Az AIA által meghatározott alapvetőjogi hatásvizsgálat esetében tehát mindenképp megállapítható az adatvédelmi tisztviselő kötelezettségének megjelenése abban az esetben, ha a magas kockázatú MI-rendszer a hivatkozott cikkben szabályozott személyes adatokat érint, és amire nézve e körben adatvédelmi hatásvizsgálat készült. Ilyetén megállapítható, hogy közvetve maga az AIA is tartalmaz feladatellátási kötelezettséget az adatvédelmi tisztviselők számára, hiszen nevezett adatvédelmi hatásvizsgálatnak kiegészített részévé kell tenni az alapjogi hatásvizsgálatot. Ez pedig- a rendelet nyelvtani értelmezését alapul véve- azt indikálja, hogy az adatvédelmi hatásvizsgálat keretrendszerét kell kiegészíteni az AIA vonatkozó rendelkezéseivel, így, ha magát az alapjogi hatásvizsgálatot nem is az adatvédelmi tisztviselő folytatja le, egyfajta ellenőrzési funkciót a két vizsgálati anyag egységesítésében el kell látnia.

4. Az emberi felügyelet szerepe és kötelezettsége

Az AIA egyik központi garanciális elemének tekinthető az MI-rendszerek vonatkozásában az úgynevezett emberi felügyelet biztosításának kötelezettsége. A humán kontroll garanciális elemként való megjelenése felveti annak kérdését, hogy az adott MI-rendszer tekintetében kötelezett szervezet meglévő kontrollszervei milyen szerepben kell, hogy megjelenjenek.[57]

Az AIA (73) preambulumbekezdése a nagy kockázatú MI-rendszerek esetében kifejti, hogy azokat „*úgy kell megtervezni és fejleszteni, hogy a természetes személyek felügyelhessék működésüket, valamint biztosíthassák rendeltetésszerű használatukat és hatásaik kezelését a rendszer életciklusa során. E célból a rendszer szolgáltatójának a forgalomba hozatalt vagy üzembe helyezést megelőzően megfelelő emberi felügyeleti intézkedéseket kell meghatároznia. Így különösen, az ilyen intézkedéseknek adott esetben garantálniuk kell azt, hogy a rendszer olyan beépített működési korlátokkal rendelkezzen, amelyeket maga a rendszer nem tud felülbírálni, és reagáljon az emberi üzemeltetőre, valamint hogy az emberi felügyeletet ellátó természetes személyek rendelkezzenek az e feladat ellátásához szükséges szakértelemmel, képzéssel és felhatalmazással”.*[58]

A Belga Adatvédelmi Hatóság (továbbiakban: BAH riport) 2024 szeptemberében kiadott egy információs füzetet, amely a mesterséges intelligencia rendszerek működését értelmezi a GDPR perspektívájából.

Az információs füzetben a BAH kiemeli, hogy mind a GDPR, mind pedig az AIA szigorú rendelkezéseket tartalmaz a személyes adatok biztonságos kezelésére

[56] GDPR 35. cikk (2) bekezdés

[57] Levitina, Anna: Humans in automated decision-making under the GDPR and AI Act. *Revista CIDOB d'Afers Internacionals* 138, 2024. 121-143. o. https://doi.org/10.24241/rcai.2024.138.3.121/en

[58] AIA (73) preambulumbekezdés

az adatkezelés teljes életciklusára vonatkozóan. A GDPR a 32. cikk (1) bekezdésében megfogalmazott a „*tudomány és technológia állása*" kitétel a technológia semlegesség talaján, a megfelelő védelmi szint mindenkori garantálását várja el az adatkezelések tekintetében. Az AIA alapul véve a GDPR által lefektetett elvárásokat, kiterjedt és komoly elvárásokat támaszt mindenekelőtt a magas kockázatú MI-rendszerek vonatkozásában, ugyanis ezek a rendszerek az adatkezelési folyamatokon túlnyúlóan is súlyos kockázatokat jeleltethetnek a természetes személyekre nézve, hiszen akár a tanító adatokban fellépő torzítások, vagy a tanító adatok manipulálása többlet kockázatot eredményezhet a természetes személyekre nézve. Ezen kockázatok kezelése érdekében az AIA preventív intézkedéseket vár el, amelyek között a kockázatelemzés és a rendszer működésének folyamatos ellenőrzésén túl megjelenik az emberi felügyelet meglétének biztosítása is. [59]

Ugyancsak kitér a BAH az automatikus döntéshozatal kérdésére. A GDPR lehetőséget biztosít arra, hogy az érintettek mentesüljenek az automatikus döntéshozatali eljárás alól, illetve kérhetik az ember által biztosított felülvizsgálatot. Az AIA a magas kockázatú MI-rendszerek tekintetében minden szereplőre kiterjedően írja elő a humánkontroll meglétét, így többek között a tanító adatok ellenőrzése, a rendszer teljesítményének mérése és felügyelete mellett a döntéshozatali folyamatba való beavatkozást is lehetővé kell tenni az emberi kontroll számára.

Külön kiemelendő az elszámoltathatóság kérdésköre, amelynek GDPR szerinti kötelezettségéről a korábbiakban már részletesen is szó esett. Az AIA nem nevesíti külön az elszámoltathatóságot, azonban átfogó kockázatkezelési rendszert vár el. A kockázatok értékelésének két folyamatlépése van. Az első, mely során az MI-rendszer kockázati besorolását kell azonosítani. Ennek eredményeképp pedig különböző szintű lépések megtétele válik szükségessé az eredmények függvényében. A magas kockázatú MI-rendszerek vonatkozásában részletesebb elemzést és alapjogi hatásvizsgálatot vár el a rendelet. Ilyen esetben átfogóbb dokumentálási kötelezettség lép érvénybe, továbbá az emberi felügyelet megfelelő biztosítását is érvényre kell juttatni.[60]

IV. Összegzés

A mesterséges intelligencia szabályozása és az általa jelentett jogi kockázatok mérséklése mind jogalkotói, mind pedig jogalkalmazói oldalon komoly kihívást jelent. Közhelyes kijelentésnek tűnhet, azonban jelen esetben valóban messzemenőkig érvényes kijelentésnek tekinthető, hogy a rendkívül gyorsan változó technológiai környezet talán sose látott feladatok elé állítja a jogalkalmazókat.

[59] Data Protection Authority of Belgium General Secretariat: *Artificial Intelligence Systems and the GDPR – A Data Protection Perspective*. Brussel, Data Protection Authority of Belgium General Secretariat, 2024.
[60] U.o.

Az AIA, hasonlóan a további „Big Five" jogszabályokhoz, kockázatalapú megközelítést vár el, felismerve és elismerve ezzel a teljeskörű, valamennyi aspektusra kiterjedő jogalkotás lehetetlenségét. Így viszont az AIA hatálya alá tartozó jogalanyokra hárul a folyamatos kockázatértékelés kötelezettsége. A megfelelés garantálása azonban nem képzelhető el a személyes adatok védelmére rendelt folyamatok és belső jogintézmények megfelelő szinkronizációja nélkül.
Mint az láthatóvá vált, az adatvédelmi tisztviselők dedikált feladatokkal rendelkeznek a különböző kockázatú MI-rendszerek jogszerűségének ellenőrzésében is. Az MI-rendszerek ugyanis éppen a természetes személyekre irányuló kiterjed hatások okán olyan kockázatot jelentenek, amelyeket a DPO-nak elkerülhetetlenül ellenőrizni és felügyelnie kell.

A hatósági joggyakorlat fog tudni majd választ adni arra a kérdésre, hogy a DPO a szervezeten belül milyen formában kell, hogy részt vegyen az MI megfelelés folyamatában, nota bene, mennyire lesz összeegyeztethető a tisztviselő és mondjuk az *AI Officer*[61] munkaköre, esetleg megállapításra kerül-e az összeférhetetlenség a két pozíció között?

Meglátásom szerint kijelenthető, hogy az adatvédelmi tisztviselőnek, amennyiben az MI-rendszer személyes adatokat is kezel, annak teljes életciklusa alatt felügyeletet kell gyakorolnia, mely feladatnak az ellenőrzésen túl ki kell terjednie az adatkezelési folyamatok elszámoltathatóságának garantálására hivatott eszközök összhangba tételére az AIA által elvárt dokumentációs kötelezettséggel épp úgy, mint az adatvédelmi eljárások MI specifikus átdolgozására. Ez természetesen többlet terhet és feladatot jelent, aminek az adatkezelő által biztosított erőforrások allokálásában is érződnie kell.

[61] Fontos megjegyezni, hogy az AIA nem tartalmaz rendelkezést egy, az érintett szervezeten belül dedikált személy vagy szervezeti egység létrehozására, amelynek feladata volna az MI-rendszerek megfelelésének garantálása. Ettől függetlenül több, mint valószínű, hogy a gyakorlat elő fog hívni ilyen pozíciókat, hiszen a komplex jogalkotói elvárások meg fogják követelni azt.