Iustum Aequum Salutare
XXI. 2025. 1. • 203–212.

A SZEMÉLYES ADATOK VÉDELME AZ MI TÉRHÓDÍTÁSÁRA TEKINTETTEL

A tiltott MI-gyakorlatok és egyes kockázatosnak tekinthető MI-rendszerek alkalmazásának adatvédelmi szempontjai

Necz Dániel*

1. Bevezető gondolatok

A mesterséges intelligencia (MI) általi adatkezelés – a technológia alkalmazásával járó számos előny mellett – jelentős kihívást jelent a személyes adatok védelme számára. Mindez különösen igaz a technológia kiterjedt, egyes szenzitívnek mondható területeken való alkalmazására. A fentiekre tekintettel maga az európai mesterséges intelligenciáról szóló rendelet[1] is meghatározza a tiltottnak tekinthető MI-gyakorlatok körét, e körbe értve a demokratikus társadalmak működése szempontjából leginkább kockázatosnak tekinthető rendszereket. A fentiek mellett további olyan MI alkalmazásokról, illetve kapcsolódó adatkezelésekről is beszélhetünk, amelyeket a jogalkotó jellemzően kockázatosnak tekint, és az érintettek jogainak és szabadságainak különös figyelembevételét követeli meg azok alkalmazóitól.[2] Így ezen alkalmazások, habár nem tekinthetők tiltottnak az MI Rendelet alapján, mégis ebbe a kategóriába eshetnek, vagy egyébként jogsértő adatkezelést valósíthatnak meg.

A fentiekre tekintettel a jelen tanulmányban a tiltott MI-gyakorlatok adatvédelmi szempontjai mellett vizsgáltuk a biometrikus azonosítás adatvédelmi kihívásait, a kockázatértékelésekhez használt MI-rendszerek, valamint a *webscraping* adatvédel-

* Jogász. ORCID: https://orcid.org/0009-0005-6176-1449

1 Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) 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, PE/24/2024/REV/1, HL L, 2024/1689, 2024.7.12. („MI Rendelet").

2 Ideértve az MI Rendelet által meghatározott nagy kockázatú MI-rendszerek körét (MI Rendelet 6. cikk).

https://doi.org/10.69695/ias.2025.1.13

mi kihívásait, mivel ezen megoldások, illetve adatkezelések jellemzően a tiltott MI-gyakorlatok alatti kivételek körébe esnek vagy bizonyos alkalmazásaik ezek határán mozognak, így napjainkban különös kihívást támasztanak a személyes adatok védelme szempontjából.

2. A tiltott MI-gyakorlatok és azok adatvédelmi szempontjai

Az MI Rendelet meghatározza azon tiltott MI-gyakorlatok körét, amelyek alkalmazása tilosnak tekinthető. E körben hangsúlyozandó, miszerint az MI-vel kapcsolatos etikai problémák jelentős hangsúlyt élveznek a jogi szabályozás területén is, e körbe értve különösen az érintettek személyes adatainak védelmét, az adatvédelmi jogok biztosítását.[3] Így a tiltott MI-gyakorlatok között olyan MI alkalmazási módokat találunk, amelyek a demokratikus társadalmakban megengedhetetlen kockázatot jelentenek, e körbe értve különösen a személyes adatok védelmére, a magánéletre, valamint egyéb alapvető jogokra és szabadságokra jelentett kockázatokat. A fentiekre tekintettel a tiltott MI-gyakorlatok körébe tartozik az alábbiak szerinti MI-rendszerek forgalomba hozatala, üzembe helyezése, illetve használata:

- Szubliminális technikák alkalmazása: olyan MI-rendszerek, amelyek adott személy tudatán kívül, vagy célzottan manipulatív vagy megtévesztő technikákat alkalmaznak abból a célból, hogy lényegesen torzítsák egy személy vagy csoport magatartását, illetve gyengítsék az érintettek döntéshozatali képességét, és számukra kárt okozzanak. Ebbe beletartozhat bármely olyan szubliminális alkotóelem (pl. képi vagy hangingerek) alkalmazása, amelyeket az érintettek nem képesek észlelni, azonban hatással bírnak rájuk, illetve egyéb döntéshozatalt csorbító, megtévesztő technikák.[4]
- Sebezhetőség kihasználása: olyan MI-rendszerek, amelyek az adott személyek bizonyos helyzetével kapcsolatos sebezhetőségét használják ki abból a célból, hogy lényegesen torzítsák egy személy vagy csoport magatartását, és számukra kárt okozzanak. Fontos hangsúlyozni, hogy a sebezhetőség nem került e körben meghatározásra az MI Rendeletben,[5] így bármely fajta sebezhetőség fentiek szerinti kihasználása tiltott MI-használatot, és így tiltott adatkezelést valósíthat meg.
- Társadalmi pontozásra használt rendszerek: olyan MI-rendszerek, amely természetes személyek vagy csoportjaik közösségi magatartása, személyes tulajdonságaik, személyiségjegyeik alapján végez értékelést vagy osztályozást, és amely ez alapján diszkriminatív módon az érintettek számára hátrányos vagy kedvezőtlen bánásmódhoz vezet.

---

[3] Luciano Floridi: Introduction to the Special Issue. The Ethics of Artificial Intelligence: Exacerbated Problems, Renewed Problems, Unprecedented Problems. *American Philosophical Quarterly,* Vol. 61., No. 4. (2024) 302. https://doi.org/10.5406/21521123.61.4.01

[4] Pók László: Felkészülés az MI Rendelet alkalmazására – 5. rész: Tiltott MI-gyakorlatok I. *GDPR Blog,* 2024.07.02, https://tinyurl.com/2jjwwykd

[5] Rostam Josef Neuwirth: Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act. 2022. 7. http://dx.doi.org/10.2139/ssrn.4261569

– Bűnözési kockázatértékeléshez használt rendszerek: olyan MI-rendszerek, amelyek – kizárólag az adott személyekre vonatkozó profilalkotás vagy személyiségjegyeik, tulajdonságaik értékelése alapján – felmérik vagy előre jelzik annak kockázatát, hogy az adott személy bűncselekményt követ el. Mindez azért is fontos, mivel a demokratikus társadalmakban kiemelt jelentőséggel bír az ártatlanság vélelme, így a büntetőjogi felelősség megállapításával járó döntések kizárólag az érintettek tényleges magatartásán és mulasztásán, nem pedig kockázatelemzésen, illetve személyiségjegyek értékelésén alapulhatnak.[6] A fenti alkalmazások körébe nem tartoznak azonban a bűnözői tevékenységhez közvetlenül kapcsolódó, objektív tények értékelését végző rendszerek, amelyek adott esetben a bűnüldöző hatóságokat segíthetik nyomozati tevékenységük során.
– Arcképek nem célzott, tömeges lekérdezése arcfelismerő adatbázis létrehozása érdekében: olyan MI-rendszerek, amelyek arcképek internetről vagy kamerarendszereken keresztüli, nem célzott lekérdezését végzik arcfelismerő adatbázis létrehozása érdekében. Hangsúlyozandó, hogy az ilyen megoldások alkalmazásának adatvédelmi szempontjai az EU-n belül és az Egyesült Államokban is jelentős figyelmet kaptak a közelmúltban. Ennek kapcsán például a ClearView AI-al szembeni eljárások jelentősnek mondhatók, amelyek során az eljáró hatóságok, illetve bíróságok adatvédelmi szempontból jogsértőnek találták a társaságok hatóságok támogatása céljára arcképgyűjtéssel és elemzéssel járó tevékenységét.[7]
– Érzelemfelismerő rendszerek használata munkahelyi, illetve oktatási környezetben. E körben hangsúlyozandó, hogy az MI-rendszerek érzelemfelismerési célú felhasználása egyéb kontextusban bár nem minősül az MI Rendelet alapján tiltott MI-gyakorlatnak, bizonyos kivételekkel, továbbra is tiltott adatkezelést valósíthat meg.
– Szenzitív adatok levezetéséhez vagy kikövetkeztetéséhez használt biometrikus kategorizálási rendszerek: olyan MI-rendszerek, amelyek természetes személyeket biometrikus adataik alapján egyénileg kategorizálnak szenzitív adatok levezetése vagy kikövetkeztetése céljából. Ezen tilalom nem terjed ki a jogszerűen megszerzett biometrikus adatok jogszerű címkézéséhez vagy szűréséhez, illetve a bűnüldözés területén való kategorizálás céljára történő felhasználására.
– Biometrikus azonosító rendszerek valós idejű, nyilvános használata bűnüldözési célból: e körbe tartozik bizonyos kivételekkel „valós idejű" távoli biometrikus azonosító rendszerek használata a nyilvánosság számára hozzáférhető helyeken

---

6 Pók i. m.

7 A francia adatvédelmi hatóság például 5,2 millió euró összegű adatvédelmi bírságot szabott ki a Clearview AI-al szemben jogsértő adatkezelés okán (ld. https://tinyurl.com/4569j5fc). Az Egyesült Államokban az ALCU nevű jogvédő szervezet indított pert a társasággal szemben, amely egyezséggel zárult 2022 májusában, amelynek eredményeként a társaság adatbázisából törölhetik magukat az érintettek Illinois tagállamban, a társaság pedig nem értékesítheti arcképadatbázisát üzleti vállalkozások és magánszervezetek részére, továbbá öt évig Illinois államban sem végezhet ilyen értékesítési tevékenységet a tagállami és helyi rendőrhatóságok részére (ld. John v. Clearview AI, Inc., 1:20-cv-03481 (District Court, S.D. New York, 2020) [66]–[86]).

> bűnüldözési célokból. Ezen tilalom nem vonatkozik eltűnt személyek, illetve bizonyos súlyos bűncselekmények áldozatainak felkutatása céljából, konkrét, jelentős és közvetlen veszély, illetve terrortámadás tényleges és valós, illetve előre látható megakadályozása, illetve bizonyos súlyos bűncselekmények elkövetőinek lokalizálása vagy azonosítása érdekében történő használatra.[8]

Ahogy a fentiekből látható, a tiltott MI-gyakorlatok jellemzően személyes adatok kezelésével járó alkalmazási módokat foglalnak magukban, tekintettel arra, hogy ezen megoldások jellemzően nagyobb kockázatokkal járnak az érintettekre, azok csoportjaira vagy magára a társadalomra és a személyes adatok védelmére. Mindez azért is fontos, mivel a fentiek szerinti MI-alkalmazások egy része a hatóságok és egyes szervezetek számára különösen hasznos lehet, azonban azok az érintettek nézve jelentős sérelmekkel járhatnak,[9] így az európai jogalkotó igyekezett a társadalmi szempontból leginkább károsnak tekinthető megoldások tilalmazására, és e körben észszerű kivételek alkalmazására. Ennek tükrében az MI Rendelet által meghatározott tiltott MI-gyakorlatok az ezen megoldások általi adatkezelések számára is tilalmat, illetve korlátokat jelentenek. Így például az adatvédelmi hatósági gyakorlat jellemzően elutasítónak tekinthető az érzelemfelismerő rendszerek alkalmazásával kapcsolatban. Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság például 2022-ben 250 millió eurós bírsággal sújtott egy bankot érzelemfelismerő rendszer alkalmazásáért, amely során a rendszer képes volt mind az ügyfelek, mind az ügyfélkapcsolati alkalmazottak érzelmeit észlelni, és az érintetteket egyedileg azonosítani.[10] E körben megemlítendő, miszerint a munkahelyi alkalmazás körében az MI Rendelet kifejezetten megtiltja az érzelemfelismerő rendszerek alkalmazását munkahelyi vagy oktatási környezetben,[11] míg annak egyéb körben alkalmazását az adatvédelmi hatósági gyakorlat jellemzően csak korlátozott mértékben teszi lehetővé, ideértve például kutatási célú vagy egészségügyi alkalmazást (például, ha a betegek érzelmi állapotának felismerésére a megfelelő egészségügyi szolgáltatás nyújtása érdekében szükség van).[12]

Kiemelendő továbbá, miszerint a fentiek szerinti kivételek körébe tartozó, illetve egyes, fentiekhez kapcsolódó, MI Rendelet által meghatározott MI-rendszerek és -alkalmazások a nagy kockázatú MI-rendszerek körébe eshetnek, amelyek kapcsán az MI Rendelet további követelményeket támaszt. Így az MI Rendelet értelmében nagy kockázatú MI-rendszernek minősülnek az egyes, uniós harmonizációs jogszabályok hatálya alá tartozó termékek, ezek biztonsági alkotórészei, illetve az ilyen jogszabályok szerinti megfelelőségértékelésnek alávetendő termékek vagy alkotórészek, illetve

---

8 MI Rendelet 5. cikk (1) bek.

9 Johann Laux – Sandra Wachter – Brent Mittelstadt: Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance,* Vol. 18., No. 1. (2022) 24.

10 NAIH-85-3/2022. sz. határozata. (57) bekezdés.

11 MI Rendelet 5. cikk (1) f) pontja.

12 Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos 5/2021. sz. közös véleménye a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról, 35. pont.

az MI Rendelet vonatkozó mellékletében meghatározott rendszerek.[13] Amennyiben tehát az adott rendszer nagy kockázatú MI-rendszernek minősül, így ennek szolgáltatója köteles az MI Rendelet ezen rendszerekre irányadó követelményeinek megfelelni, ideértve például a rendszer tervezése és fejlesztése során annak biztosítását, hogy a rendszer működése kellően átlátható legyen ahhoz, hogy az alkalmazók értelmezhessék a rendszer kimenetét és megfelelően alkalmazhassák azt.[14]

A fentieken túl hangsúlyozandó, hogy az MI Rendelet nem alkalmazandó a tudományos kutatás-fejlesztés kizárólagos céljára kifejlesztett és üzembe helyezett MI-rendszerekre vagy MI-modellekre, és azok kimenetére,[15] továbbá szintén nem alkalmazandó – a valós körülmények közti tesztelés kivételével – az MI-rendszerekkel vagy MI-modellekkel kapcsolatos kutatási, tesztelési és fejlesztési tevékenységre azt megelőzően, hogy azokat forgalomba hozzák vagy üzembe helyezik.[16] Így tehát akár egy olyan MI-alkalmazás is az MI Rendelet hatókörén kívül eshet, amelyet kutatási célból, piacra helyezés nélkül vagy azt megelőzően folytatnak (például: MI-rendszer érzelemfelismerési célú alkalmazása). Kiemelendő azonban, hogy az ilyen alkalmazások kapcsán is szükséges az adatkezelőknek az adatvédelmi jogszabályok előírásainak megfelelniük, amennyiben az alkalmazás során személyes adatok kerülnek kezelésre.

Kérdésként merül fel továbbá, hogy amennyiben az adott alkalmazás tiltottnak minősül, azonban az adott esetben mégis szükséges valamilyen nagyobb kár elkerüléséhez, úgy esetileg megengedhető-e mégis annak alkalmazása. Például egy bankrablás esetén a rendőrség alkalmazhat-e olyan szubliminális technikákat, amely a bankrablót megadásra, vagy a túszok elengedésére késztetheti? Habár ezen kivételeket az MI Rendelet nem tárgyalja, ilyen eseti kivételek alkalmazására kizárólag az irányadó emberi jogi normákkal, közösségi és tagállami jogszabályokkal összhangban kerülhet sor, kizárva a fenti megoldás széleskörű alkalmazását.[17]

3. A biometrikus azonosítás adatvédelmi kihívásai

A gyakorlatban különös kihívást jelenthet a biometrikus azonosítást megvalósító MI-rendszerek megfelelő adatvédelmi értékelésre, különösen az MI Rendelet tiltó, illetve korlátozó szabályaira tekintettel. Így a gyakorlatban, habár az MI Rendelet és az adatvédelmi hatósági gyakorlat az érintettek védelme érdekében megtiltja, illetve korlátozza ezen rendszerek bizonyos esetekben történő alkalmazását, a MI-rendszerek biometrikus azonosítás céljára szolgáló (például: arcfelismerő rendszerek) alkalmazása megengedhető lehet olyan esetekben, ahol ezt az alkalmazás körülményei és a vonatkozó kockázatok köre lehetővé teszi. Így például – megfelelő biztonsági garanciák alkalmazásával, az érintettek jogaira és szabadságaira tekintettel – megengedhető lehet

---

13 MI Rendelet 6. cikk (1)–(2) bekezdései.

14 MI Rendelet 13. cikk (1) bek.

15 MI Rendelet 2. cikk (6) bek.

16 MI Rendelet 2. cikk (8) bek.

17 Necz Dániel: *Új fajta tudás, új fajta hatalom – a mesterséges intelligencia és a személyes adatok védelme.* Doktori értekezés. Pázmány Péter Katolikus Egyetem, Jog- és Államtudományi Kar, 2024. 35.

a biometrikus azonosítás alkalmazása repülőtéri ellenőrzés során,[18] illetve a lentebb írtak szerint korlátozott esetekben, bűnüldözési célból, amennyiben a rendszer alkalmazása szükséges az adatkezelési cél megvalósításához és azzal arányos.

„Valós idejű" távoli biometrikus azonosító rendszer esetén azonban az ilyen rendszerek alkalmazására csak konkrét célszemély személyazonosságának megerősítése érdekében kerülhet sor, az alkalmazás esetén pedig különösen figyelembe kell venni a használatot eredményező helyzet jellegét, valamint az alkalmazás elmaradásából származó körülményeket, továbbá az érintettek jogaira és szabadságaira gyakorolt következményeket, azok súlyosságát, valószínűségét és mértékét.[19] Emellett az MI Rendelet további biztonsági garanciákat is rögzít a bűnüldöző hatóságok számára, ideértve a vonatkozó uniós adatbázisban történő regisztrációt,[20] illetve a tagállam igazságügyi hatósága vagy független közigazgatási hatósága által kiadott előzetes engedélyt, kellően indokolt sürgős esetet leszámítva, amely esetben az engedély utólagos beszerzése is megfelelő lehet, az engedély elutasítása esetén pedig a hatóság köteles az alkalmazást megszüntetni, annak valamennyi eredményét és kimenetét pedig törölni.[21]

A fentiekre tekintettel, amennyiben a „valós idejű" távoli biometrikus azonosító rendszer bűnüldözési célú alkalmazása az MI Rendelet tükrében megengedett, úgy arra a fenti garanciák biztosítása esetén kerülhet sor. Emellett az MI Rendelet nagy kockázatúnak minősíti általánosságban a távoli biometrikus azonosító rendszereket (azon rendszerek kivételével amelyek kizárólagos célja annak megerősítése, hogy egy adott természetes személy azonos azzal a személlyel, akinek állítja magát), az érzékeny vagy védett tulajdonságok vagy jellemzők szerint, ilyen tulajdonságokból vagy jellemzőkből levont következtetések alapján való biometrikus kategorizáláshoz való használatra szánt MI-rendszereket, valamint az érzelemfelismeréshez használt MI-rendszereket.[22] Így ezen rendszerek alkalmazása esetén szükséges a nagy kockázatú MI-rendszerek kapcsán irányadó követelményeknek való megfelelés biztosítása.

4. A kockázatértékeléshez használt MI-rendszerek

A fentebb írtakkal összhangban a gyakorlatban szintén jelentős kihívást jelentenek a kockázatértékeléshez használt rendszerek, ezek ugyanis a rendszer jellemzői és hatásai szerint tiltott, nagy kockázatú, vagy egyébként az MI Rendelet hatálya alá nem tartozó megoldásoknak is minősülhetnek. A fentebb írtak tükrében ezen rendszerek egy részének alkalmazását – a fentebb írtakkal összhangban – az MI Rendelet kifejezetten tiltja. Ilyennek minősülhetnek a valójában társadalmi pontozást megvalósító kockázatértékeléshez használt rendszerek, az egyes bűnözési kockázatértékeléshez hasz-

[18] European Data Protection Board, Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR. Version 1.1. Adopted on 23 May 2024. 34–35.

[19] MI Rendelet 5. cikk (2) bek.

[20] Uo.

[21] MI Rendelet 5. cikk (3) bek.

[22] MI Rendelet III. Melléklet 1. pontja.

nált rendszerek, illetve egyes fentebb említett biometrikus rendszerek. Mindemellett a bűnüldöző szervek által használt,[23] illetve egyes további (például alapvető magán- és közszolgáltatásokhoz kapcsolódó)[24] értékelési rendszerek is magas kockázatú MI-rendszernek is minősülhetnek. Értelemszerűen a tiltott MI-gyakorlatot megvalósító értékelési rendszerek alkalmazása adatvédelmi szempontból is jogsértést valósít meg személyes adatok kezelése esetén, míg más esetekben a nagy kockázatú MI-rendszerek és az adatvédelmi jogszabályok rendelkezései, vagy – nagy kockázatúnak nem minősülő egyéb rendszerek esetén – kizárólag az adatvédelmi jogszabályok rendelkezései lehetnek alkalmazandók, amennyiben az adott kockázatértékelési rendszert személyes adatok kezelésére használják.

Az Európai Unió Bírósága egy ügyben például egy német hitelértékeléssel foglalkozó társaság, a Schufa adatkezelését vizsgálta. A Schufa természetes személyek fennálló tartozásainak elengedésére vonatkozó, közhiteles nyilvántartásban tárolt információkat gyűjtött és tárolt, a közhiteles nyilvántartásban tárolt időszakon túl is, a saját maga által meghatározott időszakon belül. A fenti adatkezelés kapcsán a Bíróság arra a megállapításra jutott, miszerint a magánvállalatok ezen gyakorlata ellentmond a jogszerűség, a tisztességes eljárás és az átláthatóság elvének.[25] Kiemelte továbbá, hogy minél hosszabb ideig tárolják a vonatkozó adatokat a hasonló tevékenységet végző magánvállalatok, az annál nagyobb hatással bír az érintettek érdekeire és magánéletére, és így ezen információk tárolásának jogszerűségére vonatkozó követelmények is annál magasabbak kell, hogy legyenek.[26]

A fentiekre tekintettel leszögezendő, miszerint az egyes kockázatértékeléshez használt rendszerek jellemzően sokoldalú hatásokkal járnak az érintettekre nézve. Az MI-rendszerek egy része ráadásul jelentős személyre szabási képességekkel rendelkezik, így még hatékonyabb értékeléseket végezve, amely rendszerek alkalmazása így jelentős társadalomformáló erővel is bír, illetve segítségükkel az érintettek is könnyebben manipulálhatók.[27] Így ezen rendszerek kapcsán is szükséges az adatkezelőknek megfelelő kockázatkezelési intézkedéseket alkalmazniuk. Ennek során azonban az adott rendszer képességének esetleges csökkenését is szükséges figyelembe venniük (például, hogy az adatvédelmi szempontból alkalmazott egyes intézkedések csökkenthetik-e a rendszer képességeit a hibalehetőségek felismerésére).[28]

---

23 MI Rendelet III. Melléklet, 6. pont a, c, d, e.

24 MI Rendelet III. Melléklet, 5. pont.

25 C-26/22. és C-64/22. sz. egyesített ügyek, SCHUFA Holding, ítélet [EU:C:2023:958] 108. pont.

26 C-26/22. és C-64/22. sz. egyesített ügyek, ítélet, 95. pont.

27 Floridi i. m. 11.

28 Henry Fraser – José-Miguel Bello y Villarino: Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. *European Journal of Risk Regulation,* Vol. 15., No. 2. (2024) 440. https://doi.org/10.1017/err.2023.57

5. A webscraping-el kapcsolatos meglátások

A gyakorlatban további kihívásokat jelent az ún. *webscraping,* azaz az interneten (például közösségi média oldalakon vagy más weboldalakon, nyilvános adatbázisokban) található adatok tömeges lekérdezése. Hangsúlyozandó, hogy az MI Rendelet az arcképek nem célzott, tömeges lekérdezését arcfelismerő adatbázis építése céljára kifejezetten tiltott MI-gyakorlatnak tekinti,[29] egyéb tömeges lekérdezési gyakorlatok azonban nem tekinthetők önmagukban tiltottnak, hacsak egyébként nem tartoznak más, tiltott MI-gyakorlat körébe. Emellett nyilvánosan elérhető adatok MI alkalmazásával való egyes gyűjtési és elemzési megoldásai nagy kockázatú MI-rendszereknek is minősülnek, ideértve például, ha a személyes adatok gyűjtését hitelképesség értékeléséhez, hitelpontszámok megállapítására használják (kivéve a pénzügyi csalás észlelésére használt MI-rendszereket).[30] Megállapítható továbbá, hogy a *webscraping* körébe tartozó adatkezelések jelentős segítséget jelenthetnek az MI-rendszerek fejlesztése kapcsán, ugyanis a nagy mennyiségű adat gyűjtésével és feldolgozásával a vonatkozó rendszerek is pontosabbá és hatékonyabbá tehetők. Mindez természetesen jelentős adatvédelmi kockázatokkal is járhat, így a közelmúltban több adatvédelmi hatóság is foglalkozott a kérdéssel.

Az ír adatvédelmi hatóság például a közelmúltban eljárást kezdeményezett az X közösségi médiaoldal szolgáltatójával szemben, amely az unión belüli felhasználók nyilvános posztjait elemezte a Grok nevű MI megoldásának képzése céljából. A hatósági eljárás eredményeként az X végül beleegyezett a fenti tevékenység felfüggesztésébe.[31] A nyilvánosan elérhető adatok MI-rendszerek képzése érdekében való gyűjtése kapcsán ugyanakkor felmerülhet az a kérdés is, hogy a *webscraping* tevékenység végezhető-e kizárólag üzleti célból, illetve, e körben – ha abból indulunk ki, hogy az adatkezelésre az adatkezelő jogos érdeke[32] alapján kerül sor – például magánvállalkozások érdekei felülírhatják-e az érintetti érdekeket. Mindez azért is fontos, mivel a kutatási szempontú felhasználással kapcsolatban jellemzően engedékenyebbnek volt tekinthető a közelmúltbeli adatvédelmi hatósági gyakorlat, míg az üzleti célú felhasználással szemben már szigorúbb követelményeket támasztott. A holland adatvédelmi hatóság például egy korábbi állásfoglalásában akként nyilatkozott, hogy az eredeti adatkezelési cél, valamint a *webscraping* által elérni kívánt további cél jellemzően elkülönül egymástól, s ez utóbbi adatkezelés az érintettek számára jellemzően átláthatatlan marad, így jellemzően jogsértőnek tekinthető[33] (ugyanakkor ezen álláspontját a

---

29 MI Rendelet 5. cikk (1) bek. e) pontja.

30 MI Rendelet III. Melléklet 5. pont, b).

31 Data Protection Commission, The DPC welcomes X's agreement to suspend its processing of personal data for the purpose of training AI tool 'Grok', 2024.08.08. https://tinyurl.com/4h8d8cxn

32 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) 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 (általános adatvédelmi rendelet), HL L 119., 2016.5.4, p. 1–88. 04/05/2016 („GDPR") 6. cikk (1) bek. f) pontja.

33 Autoriteit Persoonsgegevens, Richtlijnen scraping door private organisaties en particulieren, 10–11. https://tinyurl.com/yc5k6zws

holland adatvédelmi hatóság az alábbi európai uniós bírósági gyakorlatra tekintettel felülvizsgálta).[34] Megemlítendő, hogy a fenti kezdeti holland gyakorlattal szemben a francia adatvédelmi hatóság már megengedőbbnek bizonyult, és megfelelő biztonsági intézkedések alkalmazására helyezte a hangsúlyt a *webscraping* során (ideértve például a megfelelő gyűjtési kritériumok előzetes meghatározását, szükségtelen adatok gyűjtésének elkerülését, illetve haladéktalan törlését).[35]

A Bíróság C-621/22. sz. ügyben hozott döntésében megerősítette, miszerint önmagában az adatkezelő kereskedelmi érdeke is tekinthető jogos érdeknek.[36] A fenti logika természetesen az MI általi adatgyűjtésre, illetve a *webscraping* megoldásokra is alkalmazható, azonban ennek során különös jelentősége van a túlzott mértékű adatgyűjtés elkerülésének, valamint az érintetti jogok védelmét biztosító intézkedések alkalmazásának. A fentiek mellett egyes MI alkalmazások esetén különösen az egymással összeférhető adatkezelések folytatásának, illetve az ún. összeférhetőségi teszt alkalmazásának lehet jelentősége. Erre olyan esetekben kerülhet sor, amikor az adatgyűjtés eredeti céljától eltérő célból is történik adatkezelés (ha az nem hozzájáruláson alapul vagy jogi kötelezettség teljesítéséhez szükséges), és a további cél az eredetivel összeegyeztethető. Ennek kapcsán az adatkezelőnek szükséges figyelembe vennie az eredeti és a további adatkezelési cél közötti esetleges kapcsolatot, az adatgyűjtés körülményeit, a személyes adatok jellegét és az adatkezelés esetleges következményeit az érintettekre nézve, valamint az adatkezeléssel kapcsolatos megfelelő garanciák meglétét.[37]

A gyakorlatban például az egyes jogszerű célok megvalósulását támogató, illetve technikai folyamatokat segítő adatkezelések tekintetében a gyakorlat megengedőbb lehet, míg az eredetitől merőben eltérő célból folytatott, illetve különösen az érintetti érdekek ellen ható adatkezelések kapcsán az adatvédelmi hatóságok szigorúbban léphetnek fel. Ugyanakkor nem jelenthető ki, hogy az eredetivel össze nem férő célból folytatott *webscraping*-tevékenység feltétlenül adatvédelmi jogsértést valósítana meg, vagy kizárólag az érintett hozzájárulása alapján lehetne folytatható. Ugyanakkor az ilyen adatkezelések jellemzően további garanciák meglétét követelhetik meg (például az adatok megfelelő anonimizálását). Megjegyzendő emellett, hogy a közösségi médiaoldalak *webscraping*-alkalmazási gyakorlata kapcsán vélhetőleg a közeljövőben is fokozott adatvédelmi hatósági figyelem várható, különösen arra tekintettel, mivel az ilyen szolgáltatók általi adatkezelések kiterjedt intenzitással és mértékben történnek. Ezen adatkezelések lényegi korlátozását napjainkban az adatvédelmi szabályok adják, azonban ez gyakran elégtelennek tűnik, így a hatékony adatvédelmi szabályozásnak és jogalkalmazásnak megfelelő tudatosságnöveléssel kell párosulnia, amely segítséget

---

34 Autoriteit Persoonsgegevens, AP: scraping bijna altijd illegaal, https://tinyurl.com/544bevdu

35 CNIL, The legal basis of legitimate interests: Focus sheet on measures to implement in case of data collection by web scraping, https://www.cnil.fr/fr/node/165906

36 C-621/22. sz. ügy Koninklijke Nederlandse Lawn Tennisbond kontra Autoriteit Persoonsgegevens, ítélet [ECLI:EU:C:2024:857] 57. pont.

37 GDPR 6. cikk (4) bek.

nyújt a felhasználóknak az adataik gyűjtésének és felhasználásnak tényleges megértéséhez.[38]

6. Záró gondolatok

A fentebb írtakkal összhangban a tiltott MI-gyakorlatok és a nagy kockázatú MI-rendszerek – ide értve a fentebb tárgyalt különös kihívást jelentő alkalmazásokat – adatvédelmi szempontjai a gyakorlatban jelentős kihívást jelentenek számos adatkezelő számára.

A fentiekre tekintettel az MI Rendelet különös hangsúlyt helyez a biometrikus azonosító rendszerek alkalmazására, különösen ideértve a bűnüldöző hatóságok általi alkalmazást, emellett tilalmakat vagy további követelményeket támaszt az egyes értékelőrendszerek kapcsán. Mindemellett a gyakorlatban egyre nagyobb hangsúlyt kapnak a *webscraping*gel kapcsolatos adatvédelmi kihívások, ideértve különösen az üzleti célokból történő adatgyűjtést és adatelemzéseket, amelyek kapcsán a jelenlegi adatvédelmi hatósági gyakorlat sem mondható egységesnek, azonban fokozott rugalmasság tapasztalható az érintetti érdekeket megfelelő módon figyelembe vevő üzleti célú felhasználásokkal kapcsolatban.

Meglátásaink szerint az összeférhetőségi teszt alkalmazása egyre jelentősebb szerepet kap majd az egyes kockázatos MI általi adatkezelések esetén, amelyek jellemzően más adatkezelésekhez kapcsolhatók vagy arra támaszkodnak, ideértve különösen a *webscraping* esetét, azonban a kockázatkezelési célú adatkezelések esetén is jelentős szempont lehet. Emellett – az adatkezelők jogos érdeken alapuló adatkezelései esetén – további kihívást jelent a jogos érdek megfelelő igazolása és dokumentálása, amely kapcsán a jogi és az informatikai szakemberek fokozott együttműködésére lesz szükséges egyes, kockázatosnak tekinthető MI-rendszerek kapcsán.

[38] Tóth András: Fogyasztóvédelmi, adatvédelmi, médiajogi és versenyjogi eszközök együttes alkalmazása, az online figyelempiacok kudarcainak kiküszöbölésére. *Infokommunikáció és Jog,* 2021/2. 12.