MTA Law Working Papers
2023/16

A mesterséges intelligenciára vonatkozó szabályozás, jogalkotás a rendvédelem tükrében

Szabó Hedvig

ISSN 2064-4515
http://jog.tk.mta.hu/mtalwp
Társadalomtudományi Kutatóközpont – MTA Kiválósági Kutatóhely
HUN-REN Centre for Social Sciences – MTA Centre of Excellence

A mesterséges intelligenciára vonatkozó szabályozás, jogalkotás a rendvédelem tükrében

Szabó Hedvig

Széchenyi István Egyetem, Állam- és Jogtudományi Doktori Iskola, PhD-hallgató
Nemzeti Közszolgálati Egyetem, címzetes egyetemi docens
szabohedv@gmail.com

Bevezető

Napjainkban a Mesterséges intelligenciával (MI) támogatott megoldásokkal az élet minden területén találkozhatunk. Döntéstámogató rendszerek segítenek bennünket a munkában, az utakon különféle autonóm funkciót használó gépjárművek haladnak el mellettünk, az esti szórakozáshoz pedig ajánló programok javasolnak sorozatokat. Mivel az MI egyre inkább átszövi a társadalom valamennyi tevékenységét, nem lehet figyelmen kívül hagyni a bűnüldözésre gyakorolt hatását sem.

Az Interpol 2022-ben megállapította, hogy fokozni kell az innovációt, hogy megoldhatóak legyen azok a biztonsági kérdések, melyeket az erősödő bűnügyi fenyegetés és a technológiai változások hoznak létre. Megállapították, hogy a rendvédelemben égető szükség van az MI felelősségteljes és etikus módon történő használatára, hogy választ tudjon adni a jelentkező bűnügyi kihívásokra.

A 21. században a bűnözők kihasználják a rendelkezésre álló technológiát, méghozzá oly módon, hogy őket nem kötik jogi keretek. Tevékenységük minimum jogelkerülésre, de még inkább jogsértésre irányul. Azaz a bűnelkövetőknek lehetősége van minden rendelkezésre álló eszközt, így a felforgató technológiákat is, bármikor, minden jogi kötöttség nélkül alkalmazni céljaik elérése érdekében.

A bűnözéssel ellentétben a rendvédelmi szervek működésének fundamentuma, hogy a jog uralma alatt, jogi keretei között látják el tevékenységüket. A rendvédelem azt és csak azt teheti meg, amit a jogszabályok előírnak. Jogon kívüli területekre nem merészkedhet, így az MI-t is ennek keretén belül fogja használni.

1. Technológiai fejlődés versus szabályozás

Nézünk végig, hogy egy új technológia megjelenésekor hogyan alakul az a szabályozás, melynek keretei között a rendvédelemnek el kell járnia. A technológiai fejlesztés kezdeti szakaszában nem lehet tudni, hogy merre halad a fejlesztés. Egyáltalán elterjed-e az innováció, vagy más hatékonyabb technológia veszi át a helyét, és ezáltal nem gyakorol érdemi hatást a társadalmi folyamatokra. Vagy ellenkezőleg, a technológia rohamosan fejlődik, megváltoztatja, átveszi más technológiák helyét és szerepét ezáltal érdemi hatást eredményez a társadalom különböző alrendszereiben. Ha a jogalkotás oldaláról vizsgáljuk a megjelenő technológiák kérdését, elsődlegesen azt kell tisztázni, hogy kell-e egyáltalán szabályozni ezt a területet. Létrejön-e egy olyan társadalmi állapot, azaz az emberek, közösségek élethelyzetében történik-e olyan módosulás, mely szükségessé teszi, hogy a megváltozott együttélési keretrendszert a jog eszközeivel rendezzük? Erre a kérdésre maga a technológia adja meg nekünk a választ a rá jellemző tulajdonságaival. Ugyanis a megjelenő technológia gazdasági, társadalmi hatásai széleskörűek meglévő értékláncok tűnnek el és újak jönnek létre.

Az MI-vel kapcsolatos eddigi tudásunk alapján kijelenthető, hogy szükség van a jogi szabályozásra. A felforgató technológia egyenesen igényli, hogy készüljenek általános jellegű, meghatározott csoportokra vonatkozó magatartási szabályok. Olyan társadalmi élethelyzetek

állnak elő, amelyek megkívánják, hogy legyenek egyértelmű igazodási pontok, vagyis, hogy egy-egy adott szituációban az egyéntől milyen magatartás az elvárható.
Miután már egyértelműen látszik a szabályozási igény, a következő lépésként azt szükséges tisztázni, hogy mikor kerüljön erre sor.
Collingridge[1] vetette fel először azt a kérdést, hogy mikor érdemes szabályozni egy új technológiát, amelyet ezért Collingridge dilemmának is neveznek. Ha a szabályozás az óvatossági elvek[2] mentén a technológiai fejlődés korai szakaszában megtörténik, ez nemcsak egy nehéz szabályozási feladat, de nagy valószínűséggel a technológia alkalmazása is lehetetlenné válik. Ugyanis ebben az időszakban nem látszik egyértelműen a technológia végleges hatása, akár még a technológia maga sem alakult ki teljesen. Ha a technológia fejlődik, illetve megjelennek a visszafordíthatatlan társadalmi hatásai, a szabályozás idejét múlttá válik, mert a hatások már érződnek, és az utólagos szabályozás pedig nem tud választ adni a már jog nélkül kezelt élethelyzetekre. A dilemma alapján ugyanakkor van egy optimális időpont, amikor meg kellene történnie a szabályozásnak, hogy az ne legyen túl korai, ezáltal akadályozva a technológia fejlődését és az avval járó társadalmi–gazdasági előnyök kihasználását, de ne legyen túl késői sem, amikor már nem lehet „a szellemet visszazárni a palackba".
Már az ipari társadalmakban is ismerünk példákat, mikor a szabályozás időpontja nem megfelelően lett megválasztva, és az óvatossági elvek mentén készült szabályozás utólag megmosolyogtató. 1865-ben a „piros zászlós törvény" előírta, hogy minden saját hajtással rendelkező jármű maximum 6 km/óra sebességgel közlekedhet, valamint három fős személyzetet is kell biztosítani, akik közül az egyik 55 méterrel a jármű előtt piros zászlót tart a kezében.
A párhuzam egyértelmű. A közlekedésben is egy felforgató technológia jelent meg, amely felülírta a régi értékláncokat, és a jogalkotás gyorsan akart reagálni az új élethelyzetre, de a nem ismerttől való félelem, a túlzott óvatosság rossz szabályozáshoz vezetett.[3] Természetesen egy 150 évvel ezelőtti jogi konstrukció nem kell, hogy elijessze a jogalkotót a 21. századi technológiák kezelésétől, hanem a cél megtalálni a legalkalmasabb időpontot és módszert a szabályozásra.
Azonban az ideális szabályozási időpont megtalálása az eltelt időszakban sem lett egyszerűbb. Az ipari társadalomból azóta információs társadalom, vagy Manuel Castells[4] szavaival élve hálózati társadalom lett, melyben a változás nemcsak annyi, hogy folyamatosan gyorsuló ütemben egyre több és jobb technológiával rendelkezünk, hanem gyökeresen megváltozott a teljes társadalom. Valamennyi társadalmi alrendszer, kapcsolathalmaz a hálózat logikáját követi, amelyek mind az új információs technológiákra épülnek.[5] A hálózatossággal összefüggő, a jogalkotási megközelítést is nagyban befolyásoló szempont, hogy az információs technológia a rugalmasságon alapul, mely megkövetelné a társadalmi reakciók, így a jogalkotás rugalmasságát is. Továbbá jellemzője a technológiáknak, hogy fokozódó konvergencia hatásuk van, amely erősen integrált rendszer kialakulásához vezet, ráadásul úgy, hogy a technológia régi, egymástól elkülönült pályagörbéi a szó szoros és átvitt értelmében is megkülönböztethetetlenné válnak.
A technológia egyre gyorsabb ütemű fejlődése újragondolásra készteti a jogalkotást az alkalmazandó eszközök tekintetében. Egy felforgató technológia által meghatározott élethelyzet kezelése megoldható-e hagyományos kötelező erővel bíró jogi eszközök (hard law)

[1] David COLLINGRIDGE: *The social control of technology* (New York: St. Martin's Press 1980).
[2] Ryan HAGEMANN - Jennifer HUDDLESTON SKEES - Adam THIERER: „Soft law for hard problems: The governance of emerging technologies in an uncertain future" *Colorado Technology Law Journal*, Vol. 17, 2018. 37.
[3] 1878-ban módosították is a jogszabályt.
[4] Spanyol szociológus, elsősorban az információs társadalom, a kommunikáció, a globalizáció kutatója.
[5] Manuel CASTELLS: „An introduction to the information age" *City*, Vol. 2, 1997. 6-16.

alkalmazásával, vagy helyette életszerűbb a nem kötelező erejű jogi eszközök (soft law)[6] használata?
Napjainkban, amikor az MI-ben hetente áttörést hozó új technológiák jelennek meg, a szabályozás központi kérdésé válik. A Collingridge-dilemma, valamint a *hard* és *soft law* alapján is érdemes vizsgálni, éppen hol jár az MI szabályozás, különösen a témánk szempontjából releváns területen, a rendvédelemben.

2. Amerikai Egyesült Államokat (USA)

2020-ban elfogadásra került[7] a nemzeti mesterséges intelligencia-kezdeményezésről szóló törvény[8] (Törvény), melynek célja volt, hogy fenntartsa az USA vezető szerepét az MI kutatások és alkalmazások területén. A jogszabály különböző témákban hozott rendelkezéseket:

- meghatározta azt a nemzeti koordinációs mechanizmust, mely széles körben segíti az MI kutatást és alkalmazást, így az oktatás, a munkaerőpiac, a szabványosítás területén is;
- létrehozta azt a hivatalt, mely fő felelőse a szövetségi szintű MI-vel kapcsolatos feladatoknak, és amely elősegíti a kutatás és szakpolitika koordinációját a szövetségi szinten belül;
- meghatározta különböző szövetségi intézmények részére MI kutatások elindítását és meglévő kutatások bővítését;
- az MI munkaerőpiaci hatásának kezelése érdekében támogatja az MI képzések, gyakorlatok szervezését;
- elvárja az MI jogi és etikai kereteinek kialakítását, mely támogatja a biztonságos, felelős és méltányos MI felhasználást;
- kiemeli a nemzetközi együttműködés fontosságát az MI kutatásban és szabályozásban, de oly módon, hogy az USA technológiai előnyének védelme megvalósuljon az MI területén;
- ösztönzi a partnerséget a közszféra, az iparág, az akadémiai terület és a nonprofit szervezetek között az MI területén.

Egyértelmű, hogy az USA a Törvénnyel nem az MI által létrejött új élethelyzeteket akarta kógens módon, általános hatállyal szabályozni, hanem egy olyan összehangolt programot hirdetett meg, mely alapján egyértelműek a célok és a feladatok az MI területén.
A Törvény a kormányzati intézményeknek kötelező iránymutatást ad, hogy egy kiemelt cél érdekében milyen tevékenységeket kell végrehajtaniuk, de az állampolgárok számára semmilyen kötelező magatartás nem kerül meghatározásra.
Az amerikai jogalkotás a Törvény hatályba lépésével nem tűzte ki célul, hogy valamilyen módon kezelje azokat a félelmeket, melyek az MI-vel kapcsolatosan egyre inkább nyilvánosságot kapnak. Így a Collingridge-dilemmában megjelenő korai, az előzőekben említett óvatosságon alapuló, mindenkire alkalmazandó kötelező normákat tartalmazó jogalkotás az MI területén egyelőre nem jellemző az USA-ra.
A hard jog területével ellentétben a soft jogban történtek előrelépések az MI kihívások megoldására. Ennek kiváltó oka volt egyrészről az is, hogy mind a tudományos közösségben, mind a közéletben egyre gyakoribbá váltak az MI veszélyeivel foglalkozó nyilvános megjelenések. A ChatGPT publikálása óta futótűzként terjedtek az MI valós, valamint némely esetben vélt kockázatairól szóló médiahírek. Ezek alapján napjainkra minden társadalmi

[6] Cynthia Crawford LICHTENSTEIN: „Hard Law v. Soft Law: Unneccesary Dichotomy?" *The International Lawyer* Vol. 35, No. 4, 2001.
[7] 2021. január 1-jén hatályba lépett.
[8] www.congress.gov/bill/116th-congress/house-bill/6216/text.

rétegben megjelent az a vélemény, hogy az MI-vel kapcsolatos kockázatok kezelése indokolt és szükséges.
Másrészről az USA – az eddigi gyakorlatához híven – technológiai keretrendszereket hozott létre, melyeknek célja a megbízható, stabil, minőség alapú működés biztosítása. Az MI vonatkozásában is ez a munkamódszer került alkalmazásra, így a Nemzeti Szabványosítási és Technológiai Intézet (NIST)[9] dolgozta ki a soft law megoldást. (A NIST a Kereskedelmi Minisztérium irányítása alatt működő intézmény, melynek egyik feladata a szabványosítás, beleérve az MI megoldásokat is.) Az MI kihívások kezelése érdekében a NIST 2023 januárjában kiadta a MI kockázatkezelési keretrendszert[10] és a kockázatkezelési szabálykönyvet.[11]
A kockázatkezelési keretrendszer megfelel a soft law kritériumoknak, mivel alkalmazása önkéntes, rugalmas, nem ágazatspecifikus, de képes választ adni az MI-vel kapcsolatos kihívásokra, és a technológia fejlődése sem akadályozza alkalmazását. A kockázatkezelési szabálykönyv hasonló elvek mentén működik, mivel célja, hogy a kockázatkezelési keretrendszerben meghatározott eredmények eléréséhez intézkedéseket javasoljon.
A Szabálykönyv nem csak abban rugalmas, hogy el lehet dönteni, hogy egyáltalán alkalmazza-e valaki, de magában a tartalmában is, mert nem egy ellenőrző listaként működik, melynek minden egyes lépését végre kell hajtani, hanem a javaslatokból is ki lehet választani és csak azokat alkalmazni, melyek illeszkednek a szervezet igényeihez. Ez alapján a javaslatok önkéntesek, és a szervezetek döntésére van bízva, hogy felhasználják-e a javaslatokat, és abból annyit alkalmaznak, amennyi az adott iparág felhasználási érdekeinek megfelel.
Az USA MI megközelítését rendvédelmi oldalról vizsgálva elmondható, hogy egyrészről bármelyik szervezethez hasonlóan a rendvédelemi szerveknek is van lehetőségük a Keretrendszer és Szabálykönyv alkalmazására, másrészről a rendvédelem különleges közjogi jellegénél fogva megkülönbözetett figyelmet kap az USA-ban is. Ezt bizonyítja, hogy a Törvény által létrehozott Tanácsadó Bizottság[12] (NAIAC) – a Kongresszus utasításának megfelelően – létrehozta a Rendvédelmi Tanácsadó Albizottságot,[13] melynek fő feladata információk és ajánlások megfogalmazása az Elnöknek, elsősorban olyan témákban, mint az MI megoldások használata a rendvédelem és nemzetbiztonság területén, oly módon, hogy az alapvető jogok, beleértve a magánélet és az adatok védelme is biztosított legyen. A Kongresszus utasította a NAIAC-ot, hogy az első év után,[14] majd háromévente készítsen jelentést az Elnöknek és a Kongresszusnak a Törvénnyel kapcsolatos megállapításairól és ajánlásairól. A Bizottság első jelentése[15] tartalmazza, hogy a jövőben a Rendvédelmi Albizottsággal közösen vizsgálják a megbízható, jogszerű MI-t és a további használat lehetőségeit.

3. Európai Unió

2018-tól kezdődően az Európa Unió (EU) jó néhány, jogi kötelező erővel nem bíró, de mindenképp meghatározó jelentőségű dokumentumot fogadott el az MI-vel összefüggésben, amelyek mutatják, hogy az EU is úgy tekint a mesterséges intelligenciára, mint amely hosszútávú gazdasági és társadalmi előnyökhöz vezethet, de megvannak a kockázatai is. Az Európai Bizottság közleményeiben rögzítette a mesterséges intelligenciára vonatkozó jövőképét, amely az „etikus, biztonságos, korszerű és Európában készült MI-t” támogatja.[16]
A Bizottság MI megközelítésében a három kulcsterület:

[9] www.nist.gov/artificial-intelligence.
[10] nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[11] airc.nist.gov/AI_RMF_Knowledge_Base/Playbook.
[12] National Artificial Intelligence Advisory Committee (NAIAC).
[13] Subcommittee on AI and Law Enforcement (NAIAC-LE).
[14] www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf.
[15] 2023. május.
[16] SWD(2018) 137 final.

- EU technológiai és ipari kapacitásainak bővítése, és a mesterséges intelligencia egész gazdaságra kiterjedő hasznosítása;
- felkészülés a társadalmi-gazdasági változásokra;
- megfelelő etikai és jogi keret biztosítása.

A Bizottság a jogi és etikai keretek előkészítése érdekében létrehozta a magas szintű mesterséges intelligencia munkacsoportot (AI HLEG), mely 2019-ben jelentette meg az első etikai iránymutatását a megbízható MI-ről,[17] majd a „szakpolitikai és befektetési ajánlások a megbízható MI érdekében"[18] című iratát. 2020 júliusára véglegesítette „az értékelési lista a megbízható MI érdekében"[19] dokumentumot az alapkövetelményeket alkalmazni kívánó MI fejlesztők és üzemeltetők számára, valamint foglalkozott a „szakpolitikai és beruházási ajánlásokkal kapcsolatos ágazati megfontolásokkal".[20] Az első közlemény után két évvel tette közzé a Bizottság a „Fehér könyv a mesterséges intelligenciáról: a kiválóság és a bizalom európai megközelítése" elnevezésű dokumentumot. Az előzőekben felsorolt kiadványok ugyan nem kötelező erejűek, ugyanakkor gyakorlati eszközt adnak a felhasználóknak (vö. értékelési lista) az értékrendi keretek meghatározására, de befolyásolják az MI európai megközelítését is, és soft lawként működnek. Az Unió jogszabályalkotási gyakorlata alapján minden tagállamnak egyértelmű, hogy az előkészület alatt lévő MI Törvény a fenti dokumentumokban lefektetett elveket fogja követni, mely erősíti azt a hatást, hogy a jogalkalmazók ezek alapján hozzanak döntéseket, még ha nem is kötelező alkalmazni őket.
De az EU nem állt meg a soft law eszközök alkalmazásánál, hanem olyan jogalkotási folyamatba kezdett, melynek egyértelmű célja, hogy általános jelleggel és kötelező hatállyal – hagyományos kötelező erejű hard law eszközként – szabályozza azokat az életviszonyokat, amelyekben megjelenik az MI.
A készülő MI Törvény jogalapja EUMSZ 114. cikke,[21] tekintettel arra, hogy a Bizottság értékelése szerint az MI-re vonatkozó javaslat az EU digitális egységes piaci stratégiájának központi eleme. Ugyanakkor a rendelet néhány speciális rendelkezése miatt[22] – a különös szabályokat illetően – az EUMSZ 16. cikke tekinthető jogalapnak. Az MI Törvény rendelet formájában kerül majd kihirdetésre, azaz az összes tagországban automatikusan és egységesen alkalmazandó, így biztosítva az egységes európai megközelítést és jogalkalmazást.
A tervezet meghatározza a mesterséges intelligencia fogalmát, fő célkitűzésként technológia-semleges megközelítésben, valamint a jogbiztonság érdekében az I. számú mellékletében felsorolja a MI rendszerek jelenleg ismert technológiáját.[23]
A mesterséges intelligencia kockázat alapú megközelítésében elkülöníti:

- a tiltott, elfogadhatatlan,

[17] op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1.
[18] digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence.
[19] digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment
[20] futurium.ec.europa.eu/sites/default/files/2020-07/Sectoral%20Considerations%20On%20The%20Policy%20And%20Investment%20Recommendations%20For%20Trustworthy%20Artificial%20Intelligence_0.pdf.
[21] Az Európai Unió működéséről szóló szerződés egységes szerkezetű változata – Harmadik rész: Az Unió belső politikái és tevékenységei - VII. cím: A versenyre, az adózásra és a jogszabályok közelítésére vonatkozó közös szabályok - 3. fejezet: Jogszabályok közelítése - 114. cikk.
[22] Így például a hozzáférhető helyeken bűnüldözési célokból történő „valós idejű" távoli biometrikus azonosítást érintő rendelkezések miatt.
[23] Gépi tanulási megközelítések, ideértve a felügyelt, a felügyelet nélküli és a megerősítő tanulást, a módszerek széles skálájának, többek között a mélytanulásnak az alkalmazásával, Logikai és tudásalapú megközelítések, beleértve a tudás megjelenítését, az induktív (logikai) programozást, a tudásbázisokat, a következtetőmotorokat, a(z) (szimbolikus) érvelést és a szakértői rendszereket; Statisztikai megközelítések, Bayes-féle becslés, keresési és optimalizálási módszerek

- a nagy kockázatú,
- a korlátozott kockázatú,
- a minimális kockázatot

jelentő rendszereket.

Elfogadhatatlan/tiltott rendszerek azok, melyek

a.) úgy sértik a személyes jogokat, hogy manipulálnak, kizsákmányolnak, kihasználják akár kiszolgáltatott, veszélyeztett csoportok, akár felnőttek sebezhetőségét, melynek eredményképp fizikai vagy pszichológiai károsodás is lehet.

b.) társadalmi scoring[24] rendszerek létrehozása, működtetése érdekében alkalmazott MI megoldások.

c.) „valós idejű" távoli biometrikus azonosító rendszereket használnak a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból (kivételek meghatározásával).

Nagy kockázatú rendszerként nyolc területet definiáltak, illetve ezeken belül is kijelölésre kerültek egyes MI rendszerek.[25]

A tanulmány témája szempontjából két területet érdemes vizsgálni.

a.) Az 1. terület a természetes személyek biometrikus azonosítását és kategorizálását határozza meg. Ezen belül a természetes személyek „valós idejű" és „nem valós idejű" távoli biometrikus azonosítására szolgáló MI-rendszereket nevesíti.

b.) A 6. terület a bűnüldözés nagy kockázatú MI rendszereit azonosítja, ide tartoznak

- az egyedi kockázat értékelő rendszerek, melyek az egyes magánszemélyeket sorolják be, hogy milyen eséllyel válnak elkövetővé vagy áldozattá;
- a poligráf és egyéb érzelmi állapot mérésére alkalmas MI alkalmazások;
- a deepfake felismerésére használt MI megoldások;[26]
- a bizonyítékok megbízhatóságának értékelésére használt MI-rendszerek;
- a profilalkotó alkalmazások, melyekben bűncselekmények előrejelzésére van lehetőség;
- a profilalkotó rendszerek, melyeket bűncselekmények felderítése, a nyomozás vagy a vádeljárás lefolytatása során használnak;
- az előre jelző rendszerek, mely Big Data alapon működnek, oly módon, hogy az adatokban megfigyelhető ismeretlen minták azonosítása vagy rejtett összefüggések feltárhatók legyenek.

A nem nagy kockázatúnak minősülő rendszerek esetében a Törvény csak minimális kötelezettséget ír elő. Az ilyen rendszereket gyártók/használók azonban dönthetnek úgy, hogy oly módon járnak el, mintha a rendszereik is nagy kockázatúak lennének, önkéntes jogkövetéssel érvényesítve minden szabályt a kockázati besorolástól függetlenül.

Az MI Törvény szabályozása figyelemmel van az általános adatvédelmi rendelet[27] és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv[28] rendelkezéseire. Mivel az MI rendszerek fejlesztésének alapja az adat, a szabályozás kitekint az adatkormányzási rendelet, a nyílt hozzáférésű adatokról szóló irányelv és az uniós adatstratégia többi kezdeményezésére is.

Vizsgálatom szempontjából nem lehet figyelmen kívül hagyni a szabályozás arányosságának kérdését sem. Az előzőekben jelzett jogalap és szubszidiaritási kérdések alapján egyértelmű, hogy a készülő rendelet a meglévő jogi keretekre épül, rendelkezései az arányos és szükséges

[24] A társadalmi scoring az állampolgárok viselkedésének pontozása és a pontokhoz joghátrányok kötése.
[25] Ld. a rendelet III. melléklete.
[26] Kelly SAYLER – Laurie HARRIS: „Deep fakes and national security" *Focus* 2020. apps.dtic.mil/sti/pdfs/AD1117081.pdf.
[27] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.).
[28] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27).

korlátozást célozza, mivel az kockázatalapú megközelítést követ. A felhasználóknak csak akkor jelent kötelezettséget, ha az MI megoldások valószínűleg nagy kockázatot hordoznak az alapvető jogok vagy a biztonság szempontjából.
A tervezet – Collingridge-dilemma alapon – a kockázat alapú megközelítést választotta, mely a mesterséges intelligenciához kapcsolódó kockázatok kezeléséhez szükséges minimum követelményekre korlátozódik avval a célkitűzéssel, hogy indokolatlanul ne korlátozza, vagy esetleg akadályozza a technológiai fejlődést, valamint ne növelje az MI alkalmazások fejlesztésének és bevezetésének költségeit, evvel versenyhátrányt okozva az Uniónak. Ebből következően a rendelet előírásait csak akkor kell alkalmazni kötelező jelleggel, ha az MI megoldás magas kockázatú.
Ezekben az esetekben a rendelet szigorú követelményként előírja

- a kiváló minőségű adatokat, dokumentációt,
- a nyomonkövethetőséget,
- az átláthatóságot, az emberi felügyeletet,
- a pontosságot,
- a megbízhatóságot,

mivel ezen feltételek megléte szükséges az alapvető jogokat és a biztonságot fenyegető kockázatok csökkentéséhez.

A Bizottság – az innovációs várakozásoknak megfelelően – megkapja a lehetőséget, hogy a rendelet III. mellékletét módosítani tudja, így a nagy kockázatú rendszerekre vonatkozó definíció naprakészen tartása megvalósítható.
Az MI Törvény tervezete a nagy kockázatú rendszerekre vonatkozóan több szintű követelményrendszert határoz meg. Egyrészről a személyi hatálya a teljesség igényével kiterjed a termékgyártókra, az importőrökre, forgalmazókra és felhasználókra, továbbá bármelyik érintett harmadik félre. Másrészről ezeknek a feleknek a nagy kockázatú MI megoldások vonatkozásában az alábbi szigorú feltételeknek kell megfelelniük:

- kockázatkezelési rendszert kell létrehozni, bevezetni, dokumentálni és fenntartani.
- az olyan MI rendszerek, melyek adatok alapján végzik a saját öntanulás/öntanításukat, tanító adatbázisnak csak a rendeletben meghatározott minőségi kritériumoknak megfelelő tanulóadat, érvényesítési adat és tesztadat készleteket használhatnak (a tanuló, tesz és érvényesítési adatnak relevánsnak, reprezentatívnak, hibáktól mentesnek és teljesnek kell lennie). Az adatkészleteket adatkormányzásnak és -igazgatásnak kell alávetni (például tisztítás, címkézés).
- az MI rendszerek műszaki dokumentációját – ennek szükséges tartalmát is egyértelműsíti a rendelet – már üzembe helyezés előtt el kell készíteni és folyamatosan naprakészen kell tartani.
- meg kell valósítani a teljeskörű naplózást (nyilvántartás).
- biztosítani kell az átláthatóságot és a felhasználók tájékoztatását.
- a rendszerek fejlesztésénél, üzemeltetésénél meg kell valósítani a pontosságot, a rendszerstabilitást és a kiberbiztonságot,
- a nagy kockázatú MI rendszerek esetén úgy kell kialakítani a rendszereket, hogy használatuk időtartama alatt természetes személyek hatékonyan felügyelhessék; ez talán a legfontosabb követelmény.

A kockázat alapú megközelítést az EP-képviselők jóváhagyták, de a tiltott mesterséges intelligencia felhasználás, gyakorlatok listáját további tilalmakkal javasolják kibővíteni, ezek tételesen:

- a valós idejű távoli biometrikus azonosítási rendszerek használata nyilvánosan helyeken (közterületeken);
- az utólagos távoli biometrikus azonosítási rendszerek használata, a bűnüldözés kivételével (a súlyos bűncselekmények üldözésére és csak bírósági engedély után);
- érzékeny jellemzőket (pl. nem, faj, etnikai hovatartozás, állampolgári státusz, vallás, politikai irányultság) használó biometrikus kategorizálásra épülő rendszerek használata;
- előrejelző rendvédelmi rendszerek (profilalkotáson, helymeghatározáson vagy korábbi bűnözői magatartáson alapulóan);
- érzelemfelismerő rendszerek a rendvédelemben, a határigazgatásban, a munkahelyen és az oktatási intézményekben;
- arcképek cél nélküli összegyűjtése (scraping) az internetről vagy térfigyelő kamera felvételekből arcfelismerő adatbázisok létrehozása céljából (sérti az emberi jogokat és a magánélethez való jogot).

A Parlament a nagy kockázatú MI rendszerek kibővítésére tett javaslatot, nevezetesen

- minden olyan MI megoldással, amely jelentős károkat okozhat az emberek egészségére, biztonságára, alapvető jogaira vagy a környezetre;
- a szavazók és a választások kimenetelének befolyásolására használt MI rendszerekkel;
- a közösségi média platformok által használt ajánlórendszerekkel (több mint 45 millió felhasználóval).

Az általános célú MI-vel kapcsolatos kötelezettségeket is megfogalmazták az EP képviselői, miszerint az alapmodellek szolgáltatóinak fel kellene mérniük, és mérsékelniük kellene a lehetséges kockázatokat. Továbbá EU-s nyilvántartásba kellene vettetniük ezeket modelleket, még az Unióba való piacra lépés előtt, és az alapmodelleken alapuló generatív[29] MI[30] rendszereknek meg kell felelniük az átláthatósági követelményeknek. Az MI szolgáltatóknak egyértelművé kell tenniük, hogy a tartalom nem ember, hanem MI által létrehozott, és biztosítaniuk kell a jogszerűtlen tartalom előállítása elleni védelmet. Amennyiben a generatív MI tanításához szerzői joggal védett adatok is felhasználásra kerülnek, részletes összefoglalót kell készíteni, amelyet nyilvánosan hozzáférhetővé kell tenni.

A bevezetőben említésre került, hogy a bűnözés minden jogi korlát nélkül használja a legújabb technológiákat, míg a rendvédelem bár szintén használhatja a legkorszerűbb alkalmazásokat, de jogi megkötöttségek mellett. Az MI Törvény hatályba lépése meg fogja ugyan változtatni a lehetőségeket, de kötöttségek a továbbiakban is maradnak.

3.1. Uniós szabályok az MI-ről a rendvédelemben

Érdemes megvizsgálni, hogy az uniós intézmények milyen álláspontot képviselnek – a készülő rendelettervezeten túl – az MI megoldások rendvédelmi alkalmazása területén.

Az EU-ban a GDPR szabályokkal egyidejűleg lépett hatályba[31] a rendvédelemre alkalmazandó az ún. bűnügyi adatvédelmi irányelv (LED),[32] amely még nem fókuszál célirányosan az MI szabályozásra, de már rögzíti, hogy természetes személyek védelme nem függhet a technológiától, azaz technológiailag semlegesnek kell lennie a védelmi megoldásoknak.

A természetes személyek védelmének akkor is érvényesülni kell, ha a személyes adatok kezelése manuális módon, vagy automatizált eszközök útján történik, de abban az esetben is érvényesíteni kell, ha a személyes adatokat nyilvántartási rendszerben tárolják vagy kívánják tárolni.

[29] Generatív jelentése: új adatok létrehozása - az előzetesen megtanított - adathalmazok/készletek felhasználásával.
[30] Pl. a ChatGPT esetében is.
[31] 2016. május 24-én lépett hatályba, kétéves türelmi időszak után 2018. május 25. után alkalmazandó.
[32] A tagállamok nemzeti jogába való átültetése megtörtént.

Az irányelv[33] egyértelműen meghatározza, hogy a rendvédelmi szervek kiknek és milyen esetekben végezhetik a személyes adatok kezelését – az általános adatvédelmi rendelettől eltérően –ezen irányelv alapján. Csak olyan feladatnál lehet alkalmazni, amelyet a hatóság bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végez. Az irányelv, hogy lehetőséget adjon a bűnüldöző hatóságok proaktív eljárásához (megelőzés) nemcsak a retrospektív szemlélet (bűnüldözés) érvényesítéséhez ad lehetőséget, hanem a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése érdekében folytatott adatkezelésekre is. A bűnügyi adatvédelmi irányelv hasonlóan az általános adatvédelmi rendelethez elkülöníti a személyes adatok különleges kategóriáit (például biometrikus adatok), amelyeknek egyre fontosabb szerepe lehetne a rendvédelmi területen.
Az irányelv a profilalkotást[34] két kategóriára bontja.
Először is, tilos azon típusú profilalkotás, mely a megkülönböztetés tilalmába ütközik, vagy amennyiben az alapjogok korlátozása[35] nem a célszerűség, a szükségesség és arányosság mentén történik. *Másodszor*, a profilalkotás egyéb eseteiben biztosítani kell az érintett számára, hogy ne terjedhessen ki rá olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amelynek célja a rá vonatkozó egyes személyes jellemzők értékelése, és amely rá nézve hátrányos joghatással járna, vagy őt jelentős mértékben érintené.
Ilyen adatkezelési esetekre megfelelő garanciák mellett kerülhet sor. Ezek a garanciák a következők:

- külön tájékoztatás biztosítása az érintettnek;
- emberi beavatkozást kérésének lehetősége, arra való válasz kötelezősége;
- az érintett álláspontjának kifejtése;
- magyarázat adása az effajta értékelés alapján hozott döntésről;
- lehetőség biztosítása az automatizált döntés elleni fellebbezésre.

A bűnügyi adatkezelésben érintett egyének védelmével kapcsolatban az Európai Adatvédelmi Testület több iránymutatást tett közzé, így legutóbb az arcfelismerő rendszerek rendvédelmi felhasználására vonatkozóan.[36] Ebben a Testület kinyilvánítja, hogy egyetértve az európai adatvédelmi biztossal, arra tesz javaslatot, hogy legyenek tiltva az alábbi arcfelismerővel kapcsolatos alkalmazási lehetőségek:

- személyek távoli biometrikus azonosítása nyilvánosan hozzáférhető helyeken;
- mesterséges intelligencia által támogatott arcfelismerő rendszerek, amelyek az egyéneket biometrikus adataik alapján sorolják kategóriákba (etnikai hovatartozás, nem, valamint politikai vagy szexuális irányultság vagy egyéb megkülönböztetési okok);
- természetes személy érzelmeinek elemzése arcfelismeréssel vagy hasonló, egyéb MI technológiával;
- a személyes adatok tömeges és válogatás nélküli feldolgozása oly bűnüldözési környezetben, amely olyan adatbázison alapul, amely online elérhető arcképek összegyűjtésével keletkezett.

[33] EU 2016/680..
[34] A személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz vagy érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.
[35] Alapjogi Charta 21. és 52. cikk.
[36] edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

Összegzés

Az MI alkalmazások megoldást jelenthetnek a rendvédelmi szerveknek, hogy új, innovatív módszereket alkalmazzanak a bűnözés elleni harcban. Míg a bűnözés szabadon használhatja a technológiát, addig a rendvédelem keretei mások, csak a jog által meghatározottan végezhetik tevékenységüket.

Világszerte megfigyelhető tendencia, hogy az MI rendvédelmi alkalmazását speciális kormányzati, jogalkotói figyelem kíséri, és egyedi megoldások születnek a rendvédelmi alkalmazások vonatkozásában. Jelenleg általános hatályú, kötelező érvényű jogszabály (hard law) nem szabályozza az MI megoldások alkalmazását, de ez nem jelenti azt, hogy nincsenek alkalmazandó/alkalmazható szabályok.

Az eltérő jogi kultúra eltérő megoldást von maga után a biztonsági területen is. Az USA-ban az Elnök közvetlen tájékoztatására hozták létre az Rendvédelmi Tanácsadó Albizottságot, mely felügyeli az MI biztonsági alkalmazásait. Ugyanakkor a szabályozás helyett a szabványosítást – mint soft law megoldást – alkalmazzák, és a NIST által kibocsátott keretrendszer és szabálykönyv alkalmas a kockázatok kezelésre.

Az Európai Unió is egyedi utat választott: előkészületben van egy általános érvényű, közvetlen hatályú MI rendelet, mely speciális szabályokat fog tartalmazni a rendvédelemben használható MI megoldásokra. De jelenleg is vannak már hatályban lévő kötelező jogszabályok, amelyek a rendvédelemben alkalmazható MI egy-egy résztevékenységét (például a profilalkotást, vagy a biometrikus adatok kezelését) szabályozzák. Ezek kötelező jogszabályként, hard lawként működnek. Eredetileg ezen jogi szabályozás technológia-semlegesként került meghatározásra, így nem az MI alkalmazásokat célozta, de jelen technológiai fejlődésnél az MI-re vonatkozik igazán. A rendelettervezet ugyanakkor célirányosan már az MI-re mint technológiára vonatkozik, szigorú tiltásokkal és korlátozásokkal. Kétség nem fér hozzá, hogy mivel a bűnügyi eszköz alkalmazások emberi alapjogi korlátozással járhatnak, szükséges minden esetben az alapjogi tesztnek megfelelően a célhoz kötöttség, a szükségesség és arányosság érvényesítése, különösen abban az esetben, ha a bűnüldözés az MI-t használja.

Az uniós kötelező hatályú rendelet tervezete jelenleg nem lezárt, így nem látjuk még, hogy véglegesen mely MI megoldások kerülnek a tiltott és a nagy kockázatot jelentő alkalmazások közé. De az irány egyértelműnek tűnik: a rendvédelmi alkalmazások egy része szigorú korlátozások alá kerül, vagy egyszerűen tiltott lesz az alkalmazása. A jogszerűségi szempontok érvényesüléséhez kiemelt érdek fűződik, hiszen a bűnügyi eszközöket alkalmazó szervek és a polgárok viszonya egyenlőtlen. Biztosítani kell az egyénnek, hogy nem lesz kiszolgáltatva a büntetőhatalomnak, alapjogai érvényesülni tudnak.

Az egyéni jogok biztosításához tartozik, hogy az egyénnek joga van a személyes biztonsághoz is. A személyes biztonsághoz való jog feltételezi, hogy a bűnüldöző hatóságoknak megfelelő eszközrendszere van a bűnözéssel szemben fellépéshez. Ez az eszközrendszer pedig azontúl, hogy alkalmas a cél elérésére, korszerű és hatékony is. A 21. században az MI az vagy lesz az a technológia, amely megfelel ennek az elvárásnak. Így a jogalkotásnak, akár hard, akár soft eszközöket alkalmaz, kettős feladata van. Egyrészről meg kell teremtenie a feltételrendszert, hogy a korlátok nélküli technológiát használó bűnözés elleni küzdelemnek is legyen megfelelő technológiája és módszertana a célirányos felhasználáshoz. Másrészről biztosítania kell az egyénnek a jogai védelmét, beleértve a biztonsághoz való jogot is. Cél az egyensúly megteremtése, meg kell találni azt a vékony határt az alapjogok rendszerében, hogy a biztonsághoz való jog ne szoruljon háttérbe a többi alapjog érvényesülése mellett. A rendvédelemnek megmaradjon az a lehetősége, hogy a technológiai újításokkal a feladat végrehajtásának hatékonyságát is tudja fokozni, és ne csak egy csonkított, olyan keretek közé szorított eszközrendszere maradjon, amelynek alkalmazása csak egy lehetőség, de nem tud valósággá válni.

MTA Law Working Papers

Kiadó: Társadalomtudományi Kutatóközpont (MTA Kiválósági Kutatóhely

Székhely: 1097 Budapest, Tóth Kálmán utca 4.

Felelős kiadó: Boda Zsolt főigazgató

Felelős szerkesztő: Kecskés Gábor

Szerkesztőség: Hoffmann Tamás, Lux Ágnes, Mezei Kitti

Honlap: http://jog.tk.mta.hu/mtalwp

E-mail: mta.law-wp@tk.mta.hu

ISSN 2064-4515