



Brüsszel, 2022. szeptember 12.
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Intézményközi referenciaszám:
2021/0106(COD)

A JOGI SZOLGÁLAT VÉLEMÉNYE¹

Küldi:	Jogi Szolgálat
Tárgy:	Javaslat – Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról – Az EUMSZ 114. és 16. cikke mint jogalapok megfelelősége a bűnüldöző és az igazságügyi hatóságokra alkalmazandó rendelkezések vonatkozásában

I. BEVEZETÉS

1. A javasolt rendelet harmonizált szabályokat állapít meg a mesterségesintelligencia-rendszerek (a továbbiakban: MI-rendszerek) Unión belüli forgalomba hozatalára és üzembe helyezésére vonatkozóan (a továbbiakban: a javasolt rendelet)².

¹ Ez a dokumentum olyan jogi véleményt tartalmaz, amely az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló, 2001. május 30-i 1049/2001/EK európai parlamenti és tanácsi rendelet 4. cikkének (2) bekezdése értelmében védett, és amelyet az Európai Unió Tanácsa nem hoz nyilvánosságra. Jogosulatlan közzététel esetén a Tanács minden jogot fenntart.

² 8115/21.

2. A távközléssel és az információs társadalommal foglalkozó munkacsoport 2022. április 7-i ülésén a Tanács Jogi Szolgálat (a továbbiakban: Jogi Szolgálat) felszólalt a mesterségesintelligencia-rendszerekről szóló javasolt rendelet kettős jogalapja (az EUMSZ 16. és 114. cikke) megfelelőségének kérdésével kapcsolatban. A Jogi Szolgálat magyarázata megerősítette, hogy az EUMSZ 16. és 114. cikke a megfelelő jogalap a javaslatához, és az EUMSZ 87. cikkének (2) bekezdése nem lenne alkalmas jogalap az EUMSZ 114. cikke helyett. A munkacsoport kérésére a Jogi Szolgálat ebben a véleményben írásban rögzíti és részletesebben kifejti a képviselője által az említett ülésen adott magyarázatot.
3. Az MI-rendszerek fogalommeghatározását a javasolt rendelet 3. cikkének 1. pontja foglalja magában. E rendszerek általánosságban bizonyos típusú szoftvereknek felelnek meg. A javasolt rendelet egyaránt vonatkozik az MI-rendszereket forgalomba hozó szolgáltatókra és az MI-rendszereket üzembe helyező szolgáltatókra. Emellett a javasolt rendelet a felhasználókra is alkalmazandó. Szolgáltató lehet az olyan természetes vagy jogi személy, vagy hatóság/szerv, aki vagy amely MI-rendszert fejleszt vagy fejlesztet, hogy azt saját neve vagy védjegye alatt forgalomba hozza vagy üzembe helyezze. Felhasználó lehet bármely olyan természetes vagy jogi személy, hatóság, ügynökség vagy egyéb szerv, aki vagy amely a felügyelete alá tartozó MI-rendszert használja.

4. A 3. cikkben szereplő fogalommeghatározások értelmében a bűnüldöző és igazságügyi hatóságok valamely MI-rendszer szolgáltatójának és/vagy felhasználójának minősülhetnek. Azok az MI-rendszerek, amelyeknek a szolgáltató által meghatározott rendeltetése a bűnüldözés vagy az igazságszolgáltatás, a III. melléklet értelmében nagy kockázatúnak minősülnek. E minőségükben alapvető követelményeknek kell megfelelniük (kockázatkezelés, tesztelés, adatkormányzás, műszaki dokumentáció, átláthatóság, emberi felügyelet, pontosság, stabilitás és kiberbiztonság), rájuk vonatkozóan bizonyos kötelezettségek vannak érvényben (például minőségirányítási rendszerek, műszaki dokumentáció, megfelelőségértékelés, korrekciós intézkedések, tájékoztatási kötelezettség, az importőrök és forgalmazók kötelezettségei), továbbá bizonyos szabványok és megfelelőségértékelés hatálya alá tartoznak. Ezek a harmonizált szabályok a (gépekről szóló) 2006/42/EK irányelvben³ és az (orvostechikai eszközökről szóló) (EU) 2017/745 rendeletben⁴ foglalt termékbiztonsági szabályokból merítenek.
5. Azok az MI-rendszerek, amelyek a nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából „valós idejű” távoli biometrikus azonosító rendszereket alkalmaznak, a tiltott MI-rendszerek kategóriájába tartoznak. Az MI-rendszerek alkalmazására vonatkozó e tilalom alól azonban vannak kivételek. Az ilyen rendszereket illetően ugyanis a tagállamok dönthetnek arról, hogy engedélyezik-e a használatukat vagy sem. Ha engedélyezik őket, akkor részletes korlátozások és biztosítékok vonatkoznak rájuk azért, hogy felhasználásukat a feltétlenül szükséges mértékre korlátozzák, valamint hogy ezáltal védjék a személyes adatok védelméhez való alapvető jogot. Ezekről a korlátozásokról és biztosítékokról a javasolt rendelet az Európai Unió működéséről szóló szerződés (a továbbiakban: EUMSZ) 16. cikke alapján rendelkezik, és azokat a nemzeti jognak kell kiegészítenie. A javasolt rendelet 5. cikke (1) bekezdésének d) pontja, valamint 5. cikkének (2), (3) és (4) bekezdése az EUMSZ 16. cikkének (2) bekezdése alapján elfogadott (a bűnüldözésben érvényesítendő adatvédelemről szóló) 2016/680 irányelvhez képest *lex specialis*-nak minősül.

³ Az Európai Parlament és a Tanács 2006/42/EK irányelve (2006. május 17.) a gépekről és a 95/16/EK irányelv módosításáról (HL L 157., 2006.6.9., 24. o.).

⁴ Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o.).

Az 5. cikk (1) bekezdésének d) pontjával összhangban e rendszerek céljai a következőkre korlátozódnak:

- i. a bűncselekmények konkrét potenciális áldozatainak célzott felkutatása, ideértve az eltűnt gyermekeket is;
- ii. természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás megelőzése;
- iii. az európai elfogatóparancsról szóló kerethatározat⁵ 2. cikkének (2) bekezdésében említett bűncselekmények elkövetőinek vagy gyanúsítottjainak felderítése, lokalizálása, azonosítása vagy büntetőeljárás alá vonása, amennyiben e bűncselekmények esetében az érintett tagállam joga szerint e tagállamban a büntetési tétel felső határa legalább háromévi szabadságvesztés vagy szabadságelvonással járó intézkedés.

Az 5. cikk (3) bekezdése értelmében az ilyen technológiáknak a bűnüldöző hatóságok általi használata igazságügyi vagy közigazgatási hatóság előzetes engedélyéhez kötendő. Kellően indokolt sürgős helyzetben azonban a rendszer használata engedély nélkül is megkezdhető, és az engedélyt elegendő a használat alatt vagy után megkérni.

Az 5. cikk (4) bekezdése értelmében a tagállamok dönthetnek úgy, hogy engedélyezik a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatát, és meghatározhatják az előzetes engedély kérelmezésére, kiadására és felhasználására, illetve az érintett bűncselekményekre vonatkozóan szükséges részletes szabályokat.

6. A javasolt rendelet jogalapja az EUMSZ 16. cikke (a személyes adatok védelme) és 114. cikke (a belső piac működése). Ezért felmerül a kérdés, hogy ezek a jogalapok megfelelők-e a bűnüldöző és igazságügyi hatóságok által szolgáltatott vagy használt MI-rendszerekre alkalmazandó harmonizált szabályok szempontjából.

⁵ A Tanács 2002/584/IB kerethatározata (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról (HL L 190., 2002.7.18., 1. o.).

7. Ez a vélemény elsőként arra összpontosít, hogy az EUMSZ 114. cikke megfelelő jogalap-e konkrétan a bűnüldöző hatóságokkal összefüggésben – amelyeket a javasolt rendelet több rendelkezése is megemlít –, azaz a nyilvánosság számára hozzáférhető helyeken alkalmazott „valós idejű” távoli biometrikus azonosító rendszerek, valamint a III. melléklet 6. pontjában említett nagy kockázatú MI-rendszerek tekintetében. Ezért azzal a kérdéssel foglalkozik, hogy az EUMSZ 87. cikkének (2) bekezdése (rendőrségi együttműködés) megfelelőbb jogalapot jelentene-e az MI-rendszereknek a bűnüldöző hatóságok általi szolgáltatására és használatára vonatkozóan, mint az EUMSZ 114. cikke (II. szakasz). E feljegyzés konklúziója analógiás módon a nagy kockázatú MI-rendszerekkel összefüggésben a III. mellékletben említett igazságügyi hatóságokra is alkalmazható.
8. Ebben a feljegyzésben megvizsgáljuk továbbá az EUMSZ 16. cikke mint további jogalap megfelelőségét, valamint a 21. és a 22. jegyzőkönyv alkalmazását a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken való, bűnüldöző hatóságok általi használatával összefüggésben (III. szakasz).

II. AZ EUMSZ 114. CIKKE MINT JOGALAP MEGFELELŐSÉGE

9. Az állandó ítélkezési gyakorlat szerint egy uniós jogi aktus jogalapja nem attól függ, hogy valamely intézmény meggyőződése szerint a jogi aktus milyen célt szolgál, hanem a jogalapot bírósági felülvizsgálatra alkalmas, objektív kritériumok – különösen az intézkedés célja és tartalma – alapján kell meghatározni. Ha egy jogi aktus vizsgálatából az derül ki, hogy az két cél elérésére irányul, vagy két összetevőt foglal magában, és ezek egyike elsődlegesnek vagy túlnyomó súlyúnak mutatkozik, míg a másik csak járulékos jellegű, a jogi aktust csak egy jogalapra kell alapítani, mégpedig arra, amelyet az elsődleges vagy döntő cél vagy összetevő megkövetel. Csak ha azt állapítják meg, hogy a jogi aktus egyidejűleg több cél elérésére irányul, amelyek elválaszthatatlanul kapcsolódnak össze úgy, hogy egymáshoz képest egyik sem másodlagos vagy közvetett, akkor lehet az ilyen jogi aktust kivételesen a különböző, vonatkozó jogalapokra alapítani, kivéve abban az esetben, ha az említett jogalapok egymással összeegyeztethetetlen eljárásokat írnak elő. Azt is meg kell jegyezni, hogy az EUMSZ 114. cikke (1) bekezdésének első mondata világossá teszi, hogy a cikk rendelkezései abban az esetben alkalmazandók, „[h]a a Szerződések másként nem rendelkeznek”. Ennek megfelelően az EUMSZ 114. cikkének alkalmazása csak abban az esetben indokolt, ha nincs másik olyan különös rendelkezés, amely a szóban forgó intézkedés elfogadásához jogalapot teremthetne⁶. Ha a Szerződés olyan konkrétabb rendelkezést tartalmaz, amely a szóban forgó intézkedés jogalapját képezheti, az intézkedésnek e rendelkezésen kell alapulnia⁷.

⁶ A Jogi Szolgálat 2016. május 17-i véleménye, 9007/16, 6. pont.

⁷ A 2004. április 29-i *Bizottság kontra Tanács* ítélet, C-338/01, EU:C:2004:253, 60. pont.

A. A JAVASOLT RENDELET CÉLJA

10. A javasolt rendelet harmonizálja egy adott szoftvertípus (MI-rendszerek) forgalomba hozatalát, üzembe helyezését és használatát. Önmagában az a tény, hogy hatóságok és magánszereplők ilyen MI-rendszerek szolgáltatói vagy felhasználói lehetnek, nem összeegyeztethetetlen az EUMSZ 114. cikkével mint jogalappal⁸.
11. Továbbá az a tény, hogy a bűnüldöző hatóságok, illetve azok, akik a nevükben eljárnak, ilyen MI-rendszerek szolgáltatói vagy felhasználói lehetnek, nem elegendő indok arra, hogy az EUMSZ 87. cikke legyen a jogalap. Meg kell vizsgálni a javasolt rendelet célját és tartalmát annak eldöntéséhez, hogy szükség van-e erre.
12. A javasolt rendelet célja általában véve az – így a nyilvánosság számára hozzáférhető helyeken alkalmazott „valós idejű” távoli biometrikus azonosító rendszerek és a nagy kockázatú MI-rendszerek tekintetében is –, hogy az egész Unióban következetes és magas szintű védelmet biztosítson, ugyanakkor megelőzze az MI-rendszerek, valamint a kapcsolódó termékek és szolgáltatások belső piacon belüli szabad mozgását akadályozó különbségeket. Egységes kötelezettségeket állapít meg az üzemeltetők számára, és garantálja a közérdeken alapuló kényszerítő indokok és a személyek jogainak egységes védelmét a belső piacon ((2) preambulumbekzdés). A javasolt rendelet konkrétan szabályokat állapít meg bizonyos MI-rendszerek forgalomba hozatalára és üzembe helyezésére vonatkozóan, ezáltal biztosítva a belső piac zavartalan működését, és lehetővé téve, hogy e rendszerek élvezhessék az áruk és szolgáltatások szabad mozgásának elvéből származó előnyöket ((5) preambulumbekzdés). Összességében a javaslat célja, hogy a tervezésétől fogva megbízható mesterséges intelligencia jöjjön létre minden ágazatban, és a mesterséges intelligencián alapuló termékek, szolgáltatások és rendszerek fejlesztésére, forgalmazására és használatára teljes körű szabályozás vonatkozzon. Tekintettel arra, hogy a mesterséges intelligenciát már számos szolgáltatás és termék keretében alkalmazzák, és ez a jövőben tovább fog terjedni, a javaslat a belső piaci logikát követi azáltal, hogy egy négy kockázati kategória köré szerveződő „termékbiztonsági keretet” határoz meg. A javaslat kötelezővé teszi a CE-jelölési eljárás lefolytatását, melynek keretében követelményeket ír elő a nagy kockázatú MI-rendszerek piacra jutására és tanúsítására vonatkozóan.

⁸ Lásd a Jogi Szolgálat jogi véleményét (ST 11395/14, 39–41. pont), valamint az olyan előzményeket, mint az (EU) 2016/2102 irányelv, valamint a 2014/24/EU, a 2014/25/EU és a 2014/23/EU irányelv.

13. A javasolt rendelet egyik meghatározott célja sem említi a közbiztonság garantálására irányuló célkitűzéseket. Még ha közvetetten teljesíteni is kell közbiztonsági célokat az MI-rendszerek bűnüldöző hatóságok általi forgalomba hozatalára/üzembe helyezésére/használatára vonatkozó harmonizálási folyamat révén, a Bíróság⁹ az EUMSZ 87. cikkének (2) bekezdését az EUMSZ 67. cikkének fényében értelmezve rámutatott arra, hogy ahhoz, hogy egy uniós jogi aktus alapját a céljára és a tartalmára tekintettel az előbbi cikk jelentse, ezen aktusnak közvetlenül kötődnie kell az EUMSZ 67. cikkben szereplő célkitűzésekhez (azaz ebben az esetben a bűnmegelőzéshez és a rendőrségi együttműködéshez). Ez a javasolt rendelettel összefüggésben kizárt, mivel az ilyen rendszerek bűnüldöző hatóságok általi használatára vonatkozó harmonizált szabályok kizárólag vagy 1. olyan termékbiztonsági típusú szabályok, amelyek az MI-rendszerek forgalomba hozatala/üzembe helyezése vagy használata tekintetében valamennyi szolgáltatóra és felhasználóra egységesen alkalmazandók, vagy 2. a személyes adatok védelmére vonatkozó szabályok, amelyekre vonatkozóan a szöveg kiegészült az EUMSZ 16. cikkével mint jogalappal (lásd alább a III. részt).
14. Egy másik ügyben¹⁰, noha a tűzfegyverekről szóló irányelv módosításának célja a közbiztonság magasabb szintjének biztosítása volt a terrorfenyegetettség és a bűnözés egyéb formái vonatkozásában, a Bíróság megállapította, hogy az áruk biztonságával kapcsolatos szempontok harmonizációja egyike a belső piac megfelelő működésének biztosítása szempontjából alapvető tényezőknek, mivel az e területre vonatkozó eltérő szabályozások alkalmasak arra, hogy kereskedelmi akadályokat képezzenek¹¹.

⁹ A 2014. május 6-i *Európai Bizottság kontra Európai Parlament és az Európai Unió Tanácsa* ítélet, C-43/12, EU:C:2014:298.

¹⁰ A 2019. december 3-i *Cseh Köztársaság kontra Európai Parlament* ítélet, C-482/17, EU:C:2019:1035.

¹¹ Ugyanott, 57. pont: „Márpedig, mivel a tűzfegyvereknek a Lengyel Köztársaság állításával ellentétben az a sajátosságuk, hogy nemcsak a felhasználók számára, hanem a széles közönség számára is veszélyt jelentenek, amint arra a Bíróság a 2018. január 23- i *Buhagiar és társai* ítélet (C- 267/16, EU:C:2018:26) 54. pontjában már rámutatott, az ezen áruk megszerzésére és tartására vonatkozó szabályozás keretében – a 91/477 irányelv (5) preambulumbekkezdésében említettek szerint – a közbiztonsági megfontolások elengedhetetleneknek tűnnek”. Lásd még: a 2018. január 23-i *Albert Buhagiar és társai kontra Minister for Justice* ítélet, C-267/16., EU:C:2018:26, 54. pont: „E tekintetben fontos megjegyezni, hogy figyelemmel arra a kockázatra, amelyet a tűzfegyverek a személyek biztonsága szempontjából jelentenek, a szabad mozgásuk csak a tagállamok közötti szállításuk feltételeinek szigorú korlátok közé szorításával érhető el, amely feltételek között szerepel az ilyen áruk szállítása által érintett tagállamok általi előzetes engedélyezés elve is”.

15. A javasolt rendeletnek a többek között az 5. cikk (1) bekezdésének d) pontjában, valamint (2), (3) és (4) bekezdésében foglalt, a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatára vonatkozó céljai, továbbá a III. melléklet 6. pontjában említett nagy kockázatú MI-rendszerekre vonatkozó rendelkezések nem kapcsolódnak közvetlenül valamely közbiztonsági célkitűzéshez. Éppen ellenkezőleg, a javaslat az azzal kapcsolatos főbb aggályokra ad választ, hogy milyen hatást gyakorolnak az MI-rendszerek az egészségre, a biztonságra és az alapvető jogokra. Ezért a vonatkozó rendelkezések közvetlenül ahhoz a célhoz kapcsolódnak, hogy – a felhasználók egészségének, biztonságának és alapvető jogainak védelme mellett – egyenlő versenyfeltételeket garantáljanak a belső piacon az MI-rendszerek forgalomba hozatala/üzembe helyezése vagy használata során.
16. A fentiek fényében a javasolt rendelet fő célja a belső piac működésének javítása az EUMSZ 114. cikke értelmében, és az EUMSZ 67. cikkében említett célok csak közvetve és járulékosan kapcsolódnak ehhez a fő célkitűzéshez.

B. A JAVASOLT RENDELET TARTALMA

17. A javasolt rendelet lényegében arra vonatkozó szabályokat tartalmaz, hogy mi szükséges egy adott termék (MI-szoftver) oly módon történő forgalomba hozatalához (vagy üzembe helyezéséhez), amely garantálja, hogy a termék biztonságos legyen és tiszteletben tartsa az alapvető jogokat. Teljes körű szabályozást határoz meg a mesterséges intelligencián alapuló termékek, szolgáltatások és rendszerek fejlesztésére, forgalmazására és használatára vonatkozóan. A javasolt rendelet nem kötelezi a bűnüldöző hatóságokat arra, hogy valamely jogszerűen forgalomba hozott MI-rendszert használjanak, és nem szabályozza közvetlenül azt sem, hogy a bűnüldöző hatóságoknak hogyan kell használniuk az ilyen MI-rendszereket. Ehelyett egyértelműen meghatározza azokat a helyzeteket, amikor a tervezett felhasználás nagy kockázatúnak minősül pusztán azért, mert egy adott MI-rendszert bűnüldöző vagy igazságügyi hatóságok fognak használni.

18. A javasolt rendelet 29. cikke egyébként szabályokat tartalmaz arra vonatkozóan, hogy milyen feltételekkel használhatók a nagy kockázatú MI-rendszerek, de ez a rendelkezés nem ágazatspecifikus, korlátozott hatályú (főként a termék használati utasítását érinti), és szervesen kapcsolódik a javasolt rendelet értelmében az MI-rendszerek fejlesztőire vonatkozó kötelezettségekhez. Emellett némi mozgásteret biztosít a tagállamoknak arra, hogy további szabályokat határozzanak meg az ilyen nagy kockázatú MI-rendszerek használatára vonatkozóan. Ami a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatát illeti (5. cikk), a javasolt rendelet adatvédelmi szempontból részlegesen szabályozza az ilyen rendszerek használatát az EUMSZ 16. cikke alapján (lásd alább a III. részt).
19. Továbbá kizárólag a tagállamok dönthetnek arról, hogy lehetővé teszik-e az ilyen „valós idejű” távoli biometrikus azonosító rendszerek teljes vagy részleges engedélyezését. Az ilyen felhasználás konkrét feltételei továbbra is a nemzeti jogban határozandók meg, ugyanakkor tiszteletben kell tartaniuk a rendeletben meghatározott következő általános kritériumokat és biztosítékokat: előzetes bírósági vagy közigazgatási engedély, az előzetes engedély kérelmezése, kiadása és felhasználása, valamint azon bűncselekmények megjelölése, amelyekkel kapcsolatban ilyen rendszerek alkalmazhatók.

20. Az MI-rendszerek a szoftverek egy meghatározott típusának minősülnek. Az MI-rendszerek forgalomba hozatalára vagy üzembe helyezésére/használatára alkalmazandó harmonizált szabályok tehát a termékbiztonsági szabályokhoz hasonló harmonizált szabályok. E szabályok egységesen alkalmazandók, függetlenül attól, hogy közsférabeli vagy magánfelhasználóról van-e szó. A javasolt rendelet idevágó preambulumbekzdései szerint ezért az egész Unióban következetes és magas szintű védelmet kell biztosítani. Ugyanakkor meg kell előzni az MI-rendszerek, valamint a kapcsolódó termékek és szolgáltatások belső piacon belüli szabad mozgását akadályozó különbségeket. Ennek érdekében az üzemeltetők számára egységes kötelezettségeket kell megállapítani, és az EUMSZ 114. cikke alapján garantálni kell a közérdeken alapuló kényszerítő indokok és a személyek jogainak egységes védelmét a belső piacon¹².
21. A javasolt rendeletnek a nagy kockázatú MI-rendszerekről szóló III. melléklete számos ponton hivatkozik a bűnüldözésre, a határellenőrzés irányítására és az igazságszolgáltatásra (6., 7. és 8. pont). Ezen pontok részletes és kimerítő felsorolást tartalmaznak a 6. cikk (2) bekezdésének megfelelően, a 6. cikk (1) bekezdésében említett, a termékbiztonsági kockázatokhoz kapcsolódóan nagy kockázatúként besorolt más rendszereken túlmenően. A 6. cikk (1) bekezdése szerint lényegében bizonyos MI-rendszerek jellegükénél fogva nagy kockázatúnak tekintendők amiatt, hogy az alapvető jogokra, az egészségre vagy a biztonságra nézve várhatóan komoly és nagy kockázatot jelentenek. A III. mellékletben felsorolt, nagy kockázatúnak tekintett egyéb rendszerek közé tartoznak az oktatás, a kritikus infrastruktúrák irányítása, a foglalkoztatás, a biometrikus azonosítás és kategorizálás, valamint az alapvető köz- és magánszolgáltatásokhoz való hozzáférés területén alkalmazott rendszerek.

¹² Ezért a mesterséges intelligencia belső piacon történő fejlesztésének, használatának és elterjedésének elősegítése érdekében szükség van a mesterséges intelligenciára vonatkozó harmonizált szabályokat meghatározó uniós jogi keretre, amely ugyanakkor garantálja a közérdek – például az egészség és a biztonság – magas szintű védelmét, valamint az alapvető jogok védelmét, amelyeket az uniós jog elismer és véd. E célkitűzés elérése érdekében szabályokat kell megállapítani bizonyos MI-rendszerek forgalomba hozatalára és üzembe helyezésére vonatkozóan, ezáltal biztosítva a belső piac zavartalan működését, és lehetővé téve, hogy e rendszerek élvezhessék az áruk és szolgáltatások szabad mozgásának elvéből származó előnyöket (lásd a javaslat (2) és (5) preambulumbekzdését).

22. A nagy kockázatú MI-rendszerekre vonatkozó ezen szabályok azonban azt nem írják elő, hogy a bünyldöző és az igazságügyi hatóságok (vagy a meghatározott területeken működő egyéb hatóságok) használhatnak-e ilyen rendszereket vagy sem. A javasolt rendelet csak közvetve fog hatást gyakorolni azon MI-rendszerek tényleges fejlesztésére, amelyeket a bünyldöző hatóságok esetleg használhatnak, valamint a jelenleg, illetve a jövőben használt MI-rendszerekre. A szabályok tehát olyan MI-rendszerekre vonatkoznak, amelyek „rendeltetése” az említett hatóságok általi használat (ld. a 3. cikk 12. pontját, a 8. cikk (2) bekezdését és a III. mellékletet). Amennyiben egy adott MI-rendszert nagy kockázatúként sorolnak be, azzal a következménnyel jár, hogy meghatározott szabályrendszert kell alkalmazni rá a kockázatkezelés, az adatkormányzás és a műszaki előírások tekintetében. Az ilyen nagy kockázatú MI-rendszerek felhasználóinak be kell tartaniuk a használati utasításokat, naplót kell vezetniük, és adatvédelmi hatásvizsgálatot kell lefolytatniuk.
23. Ezen túlmenően, a használati utasításokkal kapcsolatos felhasználói kötelezettségeken kívül egyéb felhasználói kötelezettségeket is előírhat az uniós vagy a nemzeti jog, mégpedig a felhasználó arra vonatkozó mérlegelési jogkörének sérelme nélkül, hogy a szolgáltató által megjelölt emberi felügyeleti intézkedések végrehajtása céljából megszervezze saját erőforrásait és tevékenységeit (a javasolt rendelet 29. cikkének (2) bekezdése). Ezek a szabályok további alapjogi biztosítékokat nyújtanak a nagy kockázatú MI-rendszerek tekintetében.

24. A fentiek fényében hangsúlyozni kell, hogy a javasolt rendelet nem tartalmaz arra irányuló szabályokat, hogy a forgalomba hozott nagy kockázatú MI-rendszerek használatát engedélyezzék, vagy éppen megtiltsák a bűnüldöző hatóságok számára. A javasolt szabályok értelmében a bűnüldöző hatóságok által kifejlesztett vagy használt MI-rendszerek külön kategóriát képeznek majd (nagy kockázatú) azok tervezett használata miatt. Az ilyen felhasználást a nemzeti jog szabályozná, illetve bizonyos mértékig maguk a bűnüldöző hatóságok döntenének arról. A javasolt rendelet valójában csak minimumfeltételeket állapít meg a nagy kockázatú MI-rendszerek – köztük a III. melléklet 6., 7. és 8. pontjában felsoroltak – használatára vonatkozóan a 29. cikkben (a használati utasításokra korlátozódóan), melyeket a nemzeti jog fog kiegészíteni. Ezért különbséget kell tenni – a Bíróság ítélkezési gyakorlatával összhangban – egyrészt a javasolt rendelet szándékolt célja (amely nem az, hogy szabályozza az MI-rendszerek bűnüldöző hatóságok általi használatát), másrészt a javasolt rendelet olyan joghatásai között, amelyeket közvetve előidézhet¹³, melyek irrelevánsak a jogalap megfelelőségének elemzése szempontjából.
25. A 6., 7. és 8. pont (bűnüldözés, migráció, illetve igazságszolgáltatás) nem kiemelt területek a nagy kockázatú MI-rendszerek szempontjából. A javasolt rendelet értelmében nem feltétlenül csak azok az MI-rendszerek minősülnek nagy kockázatúnak, amelyeket a III. melléklet felsorol. Valójában a legtöbb nagy kockázatú rendszer a javasolt rendelet 6. cikke (1) bekezdésének a) és b) pontjában általános jelleggel (a termékbiztonsággal összefüggésben) felsorolt rendszerek közé tartozik. A III. melléklet egyéb nagy kockázatú MI-rendszereket is felsorol, mégpedig az 1. pontban (biometrikus azonosítás), a 2. pontban (kritikus infrastruktúra), a 3. pontban (oktatás és szakképzés) és a 4. pontban (foglalkoztatás, a munkavállalók irányítása és az önfoglalkoztatáshoz való hozzáférés), melyek mindegyike a bel- és igazságügytől (IB) eltérő területhez kapcsolódik. Az ilyen nagy kockázatú MI-rendszerek valamennyi felhasználójára egységes szabályrendszer vonatkozik, melyet nem az egyes felhasználók konkrét jogállása alapján határoztak meg (például hogy gazdasági szereplőről vagy hatóságról van-e szó), hanem az egészség, a biztonság és az alapvető jogok védelmének szemszögéből.

¹³ Lásd: a Bíróság 2018. június 21-i *Lengyel Köztársaság kontra Európai Parlament, az Európai Unió Tanácsa* ítélete, C-5/16, EU:C:2018:483, 63–68. pont, és a Bíróság 2022. június 22-i *Leistritz AG kontra LH* ítélete, C-534/20, EU:C:2022:495, 28. pont.

26. A javasolt rendelet tehát harmonizált szabályokat tartalmaz az MI-rendszerek forgalomba hozatalára, üzembe helyezésére és használatára vonatkozóan, függetlenül attól, hogy e rendszereket magánszereplők vagy hatóságok – többek között járulékosan¹⁴ bűnüldöző vagy igazságügyi hatóságok – használják-e.
27. Eltekintve a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatától, amelyre az adatkezelés tekintetében külön szabályok alkalmazandók (lásd a lenti III. szakaszt), a javasolt rendelet nem tartalmaz harmonizált szabályokat a nagy kockázatú MI-rendszerek használatára vonatkozóan. Amint azt a fenti 18. és 19. pontban kifejtettük, a nagy kockázatú MI-rendszerek használatára való hivatkozás alapvetően a termék használati utasításaira vonatkozik (29. cikk), és a fejlesztőket terhelő kötelezettségekhez kapcsolódik. Ahogy arra a 22. pontban rámutattunk, a nemzeti jog és a nemzeti hatóságok döntenek arról, hogy a bűnüldöző vagy igazságügyi hatóságok használhatnak-e egy adott, a javasolt rendelet alapján jogszerűen forgalomba hozott, nagy kockázatú MI-rendszert.
28. Ezért az EUMSZ 87. cikkének (2) bekezdése, konkrétan annak a) pontja nem megfelelő jogalap a javasolt rendelethez. A javaslatban foglalt szabályok sem nem akadályozzák, sem nem mozdítják elő a releváns információk összegyűjtését, tárolását, feldolgozását, elemzését és cseréjét. Mindössze csak annyit írnak elő, hogy amikor a bűnüldöző hatóságok ilyen tevékenységeket végeznek, a felhasználók jogainak védelme érdekében teljesíteniük kell bizonyos általánosan érvényes harmonizált feltételeket. Továbbá a közös nyomozási technikák kidolgozása sem szerepel a javasolt rendeletben meghatározott célok között. A nagy kockázatú MI-rendszerek használatát illetően javasolt követelmények nem kifejezetten a bel- és igazságügy területére vonatkoznak, és nem az EUMSZ-ben meghatározott, szoros értelemben vett rendőrségi együttműködést érintik.

¹⁴ Lásd: a Bíróság A-1/19 *Isztambuli Egyezmény* véleménye, EU:C:2021:198, különösen a 298. és 301. pont.

29. Mindazonáltal a javasolt rendelet 5. cikkének (4) bekezdése értelmében a tagállamok dönthetnek úgy, hogy engedélyezik a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használatát. Amennyiben egy tagállam így dönt, köteles meghatározni az előzetes engedély kérelmezésére, kiadására és felhasználására vonatkozó, szükséges részletes szabályokat, valamint azt is, hogy milyen bűncselekményekkel kapcsolatos nyomozások és vádhatósági eljárások esetében engedélyezett e használat¹⁵. A Tanácson belül folytatott megbeszélések eredménye alapján ezek a javasolt szabályok nem ruháznák fel új hatáskörökkel az érintett nemzeti hatóságokat. Ehelyett inkább körülhatárolják a már meglévő, illetve lehetséges jövőbeli mechanizmusok alkalmazását a magánélet és a személyes adatok védelme érdekében.
30. A fentiek fényében az EUMSZ 114. cikke az egyedüli megfelelő jogalap a nagy kockázatú MI-rendszerekre – köztük a bűnüldöző és igazságügyi hatóságok által használtakra – vonatkozó harmonizált szabályokhoz, és az EUMSZ harmadik részének V. címében foglalt semmilyen bel- és igazságügyi jogalap, így az EUMSZ 87. cikke sem nem indokolt és nem is megfelelő ezen harmonizált szabályok tekintetében.

¹⁵ Megjegyzendő, hogy a javaslat 5. cikkének (4) bekezdése és a 2002/58/EK elektronikus hírközlési adatvédelmi irányelv 15. cikkének (1) bekezdése bizonyos hasonlóságokat mutat. Konkrétan, a javaslat lehetőséget biztosít a tagállamoknak arra, hogy az uniós jogban meghatározott bizonyos tilalmaktól eltérjenek. Az állandó ítélkezési gyakorlat alapján a szóban forgó tilalomtól való eltérést lehetővé tevő nemzeti rendelkezéseknek szükségszerűen az uniós jog hatálya alá kell tartozniuk, amely pedig maga után vonja a Charta alkalmazását e rendelkezések tekintetében.

III. AZ EUMSZ 16. CIKKÉNEK MINT KIEGÉSZÍTŐ JOGALAPNAK A MEGFELELŐSÉGE

31. A javasolt rendelet jogalként hivatkozik az EUMSZ 16. cikkére; a személyes adatoknak a bűnüldözés területén való kezelése tekintetében a (25) és (26) preambulumbekkezdése hivatkozik a 21. jegyzőkönyv 6a. cikkére és a 22. jegyzőkönyv 2a. cikkére, amelyek a személyes adatoknak a bűnmegelőzés területén való kezelésére vonatkoznak. A Bizottság véleménye szerint az EUMSZ 16. cikke kizárólag a biometrikus személyes adatok kezelésére vonatkozó korlátozásokat előíró rendelkezések jogalapjaként szolgál, a 2016/680 irányelvhez (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv) képest kiegészítő módon. Az 5. cikk (1) bekezdésének d) pontja főszabály szerint tilalmat ír elő, amely alól három esetben lehet kivételt alkalmazni. Konkrétan, tilos a „valós idejű” távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából történő használata, kivéve ha az a) bűncselekmények potenciális áldozatainak célzott felkutatása, b) természetes személyek életét vagy fizikai biztonságát fenyegető közvetlen veszély, illetve terrortámadás megelőzése, c) súlyos bűncselekmények elkövetőinek vagy gyanúsítottjainak lokalizálása, azonosítása vagy büntetőeljárás alá vonása (utalás az európai elfogatóparancsra) céljából feltétlenül szükséges. Az 5. cikk (2), (3) és (4) bekezdése további feltételeket szab az MI-rendszerek bűnüldöző hatóságok általi, fent említett konkrét használatára vonatkozóan, nevezetesen a következőket: értékelni kell a használat szükségességét és arányosságát, azt előzetesen engedélyeztetni kell (a vészhelyzetek kivételével), valamint a tagállamokat illeti meg az a döntés, hogy ilyen helyzetekben nemzeti szinten engedélyezik-e az MI-eszközök ezen konkrét használatát.
32. Az 5. cikk az MI-eszközök konkrét használatát részletesen szabályozó olyan rendelkezés, amely nemcsak a meglévő uniós jogszabályi keret (a szintén az EUMSZ 16. cikkén alapuló, a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv) kiegészítését célozza, hanem előírja egy nemzeti végrehajtási keret meglétét is.

33. Lényegét tekintve az 5. cikkben foglalt különös szabály – annak ellenére, hogy tilalomként fogalmazták meg – úgy tekinthető, hogy az az egyének nyilvános helyeken való, azonosításuk céljából MI-eszközökkel történő „valós idejű” általános megfigyelésére vonatkozóan szigorú szabályokat és kivételeket állapít meg. A tilalom is tágabb körű, mint pusztán a felvételt készítő kamerák használatának megtiltása, és az MI-eszközöknek a nyilvánosság számára hozzáférhető helyeken történő, az emberi jellemzők (például arcok, ezenfelül többek között a járás, ujjnyomatok, DNS, hang, gépelési dinamika, illetve egyéb biometrikus jelek és viselkedésminták) automatikus felismerését célzó használatára utal. Ebben beleértendő az adatrögzítés és az azzal egyidejű személyazonosítás is összehasonlító elemzés/adatellenőrzés révén. Ezenkívül erre a szabályra többek között annak fényében kell tekinteni, hogy nyilvános helyeken engedélyezett lehet a magánfelhasználók általi „valós idejű” azonosítás is (például labdarúgó-mérkőzéseken és hasonló eseményeken).
34. A Bizottságtól kapott további felvilágosítás alapján úgy tűnik, hogy jelenleg nincs olyan tagállam – vagy esetleg elenyésző számú olyan tagállam van –, amely szabályozza ezt a konkrét kérdést abból a célból, hogy engedélyezze a bűnüldöző hatóságok számára MI-eszközök nyilvános helyeken történő, egyének valós idejű felderítése céljából való használatát. Gyakorlati szempontból azonban annak ellenére, hogy nem mutattak fel megalapozott bizonyítékot arra vonatkozóan, hogy a meglévő gyakorlatokat és eszközöket szükséges lesz megváltoztatni, egyértelműnek tűnik, hogy a jövőbeli nyomozási technikákba, kriminalisztikai módszerekbe, valamint a bizonyítékok összegyűjtésére vonatkozó szabályokba be kell majd építeni a fent vázolt, tilalomra és kivételekre épülő megközelítést.
35. Ami a jogalapot illeti, úgy tűnik, hogy a biometrikus személyes adatok kezelését (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvhez képest) kiegészítő jelleggel korlátozó rendelkezések célja a személyes adatok védelme megfelelő biztosítékok elrendelése révén. Ez a célkitűzés elválaszthatatlanul összefonódik az EUMSZ 114. cikkének hatálya alá tartozó rendelkezések célkitűzésével, oly módon, hogy egyik célkitűzés sem másodlagos a másikhoz képest, és nem közvetett a kapcsolatuk. A javasolt rendelet célja, hogy kockázatalapú megközelítést követve általános keretet állapítson meg a mesterségesintelligencia-rendszerekre vonatkozóan. Ebben az összefüggésben az MI-rendszerek horizontális szabályozása magában foglalhat olyan szigorú biztosítékokat, amelyek a „valós idejű” felderítésre szolgáló ezen konkrét MI-rendszerre alkalmazandók. A személyesadat-védelemre vonatkozó megfelelő biztosítékokkal rendelkező ilyen konkrét MI-rendszer ezért elválaszthatatlanul kapcsolódik a belső piac működésének javítására irányuló általános célkitűzéshez, és ahhoz képest nem másodlagos, és nem is közvetett a kapcsolatuk. A javasolt rendeletet ezért kettős jogalapra kell alapozni az idevágó ítélkezési gyakorlattal összhangban (lásd a fenti 9. pontot).

36. Mindazonáltal továbbra is fennáll a kérdés, hogy melyik jogalap alkalmazandó a javasolt rendelet 5. cikke (1) bekezdésének c) pontjától a (4) bekezdéséig említett rendszerek használata során való személyesadat-kezelés szabályozására. Az EUMSZ 87. cikke (2) bekezdésének a) pontja a bűnüldöző szolgálatok által a bűncselekmények megelőzéséhez, felderítéséhez, nyomozásához és büntetőeljárás alá vonásához kapcsolódóan folytatott, a releváns információk összegyűjtését, tárolását, feldolgozását, elemzését és cseréjét érintő intézkedésekhez képez jogalapot.
37. Amint azt a főtanácsnok a PNR Kanada véleményben (A1/15) kifejtette, egyrészt az EUMSZ 16. cikke, másrészt az EUMSZ 87. cikke (2) bekezdésének a) pontja, illetve az EUMSZ 82. cikk (1) bekezdésének d) pontja között nem állhat fenn „*lex generalis – lex specialis*” típusú hierarchikus kapcsolat¹⁶. Az EUMSZ 16. cikkének (2) bekezdése az egyetlen olyan rendelkezés, amely az egyének védelmére vonatkozó szabályokra alkalmazandó olyan esetekben, amikor a tagállamok bűnüldöző hatóságai a személyes adataikat kezelik bűnmegelőzési célú tevékenységeik során. Az a pusztán tény, hogy az 5. cikk hivatkozik az európai elfogatóparancsról szóló kerethatározatban felsorolt súlyos bűncselekményekre, nem változtat ezen az értékelésen: ez a hivatkozás nem jelenti azt, hogy a tanácsi kerethatározatot itt alkalmazni kell.¹⁷ Ez mindössze egy jogalkotási technika a súlyos bűncselekmények felsorolására úgy, hogy ne kelljen külön mellékletet létrehozni.
38. Továbbra is fennáll az a tény, hogy az 5. cikkben megállapított szabály nem arra irányul, hogy az érintett bel- és igazságügyi intézkedések alkalmazására vonatkozó feltételeket jobban körülhatárolja, hanem annak biztosítására, hogy a jövőben a „valós idejű” biometrikus azonosítás MI-rendszerek általi alkalmazása során minden esetben megfelelően kezeljék az alapjogi aggályokat, valamint elsősorban az aziránti igényt, hogy a biometrikus adatok gyűjtése és kezelése a magánélet és a személyes adatok védelmének tiszteletben tartásával történjen.

E tekintetben a rendeletnek nem célja egy új, kötelező, kifejezetten a bel- és igazságügy területén alkalmazandó eljárás kialakítása, ehelyett kipróbált és jól bevált eljárási eszközökre támaszkodik az alapjogok tiszteletben tartásának biztosítása érdekében.

¹⁶ Lásd: Paolo Mengozzi főtanácsnok 2016. szeptember 8-i 1/15 *A Kanada és az Európai Unió közötti megállapodás tervezete* véleménye, EU:C:2016:656, 112–120. pont.

¹⁷ A súlyos bűncselekmények e listájának tagállamok általi végrehajtásáról lásd: a Bíróság 2022. június 21-i *Ligue des droits humains kontra Conseil des ministres* ítélete, C- 817/19, EU:C:2022:65, 150–152. pont.

39. Amennyiben az EUMSZ 16. cikke megfelelő kiegészítő jogalap, az kérdéseket vet fel a 21. jegyzőkönyv 6a. cikkének, illetve a 22. cikk 2a. cikkének alkalmazását illetően. Amint azt a javaslat (25) és (26) preambulumbekzdése részletezi, ez azt jelenti, hogy amikor Írországban vagy Dániában a bñüldözö hatóságok „valós idejű” távoli biometrikus azonosító rendszereket használnak a nyilvánosság számára hozzáférhető helyeken bñnmegelőzési céllal, és Írországot vagy Dániát nem kötik a rendörségi együttműködésre és a büntetőügyekben folytatott igazságügyi együttműködésre vonatkozó releváns szabályok, e két tagállamot a javasolt rendelet 5. cikke (1) bekezdésének d) pontja, valamint (2) és (3) bekezdése sem köti. Ez nem jelenti azt, hogy az 5. cikk (1) bekezdésének d) pontja, valamint (2) és (3) bekezdése szabályokat tartalmaz a rendörségi együttműködésre, például a bñüldözö hatóságok közötti információmegosztásra vonatkozóan. Ez mindössze azt jelenti, hogy a javasolt rendelet 5. cikke (1) bekezdésének d) pontja, valamint (2) és (3) bekezdése – hasonlóan a 2016/680 irányelvhez (a bñüldözésben érvényesítendő adatvédelemről szóló irányelv), amely az EUMSZ 16. cikke alapján elfogadott *lex generalis* – csak a biometrikus személyes adatok kezelését szabályozza a nyilvánosan hozzáférhető helyeken bñnmegelőzési céllal alkalmazott, „valós idejű” távoli biometrikus azonosító rendszerek konkrét esetében. A bizottsági javaslat e tekintetben az uniós jogalkotó által a bñüldözésben érvényesítendő adatvédelemről szóló irányelvben megtartott megközelítést követi, és ezáltal megerősíti, hogy az EUMSZ 87. cikke (2) bekezdésének alkalmazása ebben az összefüggésben nem indokolt.
40. Az EUMSZ 114. cikkének az EUMSZ 16. cikkével való kiegészítését ebben az esetben az indokolja, hogy az 5. cikk (1) bekezdésének d) pontja, valamint (2) és (3) bekezdése azok az egyedüli rendelkezések, amelyek olyan engedélyezett MI-rendszer használatát szabályozzák, amely ütközik a személyes adatok védelméhez való joggal, ez pedig *lex specialis* az általános adatvédelmi keret tekintetében. A szóban forgó érzékeny MI-rendszerek használatát érintő ilyen *lex specialis* adatvédelmi szabályok nem tekinthetők másodlagosnak vagy közvetettnek a belső piaci jogalaphoz képest. Ezért a javasolt rendelet jogalapjának az EUMSZ 16. cikkével való kiegészítése kellően indokolt, az EUMSZ 87. cikke (2) bekezdésének a) pontjára való hivatkozás pedig nem megfelelő.

IV. KONKLÚZIÓ

41. A fentiekre figyelemmel a Tanács Jogi Szolgálatának a véleménye a következő:

- a) az EUMSZ 16. és 114. cikkére mint a javasolt rendelet jogalapjára való hivatkozás indokolt és megfelelő;
 - b) az EUMSZ 87. cikke (2) bekezdésének a) pontjára vagy bármely más bel- és igazságügyi jogalapra való hivatkozás nem indokolt és nem megfelelő a bűnüldöző vagy igazságügyi hatóságok által szolgáltatott vagy használt MI-rendszerekre alkalmazandó harmonizált szabályokkal kapcsolatban.
-