European Data Protection Board

EDPS

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

2021. június 18.

Összefoglaló

2021. április 21-én az Európai Bizottság a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatot (a továbbiakban: javaslat) terjesztett elő. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli a jogalkotónak a mesterséges intelligencia (MI) Európai Unión (EU) belüli használatával kapcsolatos aggályait, és hangsúlyozza, hogy a javaslatnak kiemelkedően fontos **adatvédelmi vonatkozásai** vannak.

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos megjegyzi, hogy a javaslat **jogalapja** elsősorban az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikke. Emellett a javaslat az EUMSZ 16. cikkén is alapul, amennyiben az a személyes adatok kezelése vonatkozásában az egyének védelmére vonatkozó konkrét szabályokat tartalmaz, nevezetesen korlátozza az MI-rendszerek használatát a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból történő „valós idejű” távoli biometrikus azonosítás terén. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos emlékeztet arra, hogy az Európai Unió Bíróságának (EUB) ítélkezési gyakorlatával összhangban az EUMSZ 16. cikke megfelelő jogalapot biztosít akkor, ha a személyes adatok védelme képezi az uniós jogalkotó által elfogadott szabályok egyik célját vagy lényegi összetevőjét. Az EUMSZ 16. cikkének alkalmazása azt is maga után vonja, hogy – amint azt az Európai Unió Alapjogi Chartájának 8. cikke is előírja – **biztosítani kell** a személyes adatok kezelésére vonatkozó követelmények **tiszteletben tartásának független felügyeletét**.

A javaslat hatályát illetően az Európai Adatvédelmi Testület és az európai adatvédelmi biztos határozottan üdvözli, hogy az kiterjed az MI-rendszerek uniós intézmények, szervek vagy ügynökségek általi biztosítására és használatára. **A nemzetközi bűnüldözési együttműködésnek a javaslat hatálya alóli kizárása** mindazonáltal komoly aggályokat vet fel az Európai Adatvédelmi Testületben és az európai adatvédelmi biztosban, mivel ez a kizárás a kijátszás jelentős kockázatával jár (például olyan harmadik országok vagy nemzetközi szervezetek, amelyek az EU-beli hatóságok által használt nagy kockázatú alkalmazásokat működtetnek).

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **üdvözli** a javaslat alapjául szolgáló **kockázatalapú megközelítést**. E megközelítést azonban pontosítani kell, az „alapvető jogokra jelentett kockázat” fogalmát pedig összhangba kell hozni az általános adatvédelmi rendelettel és az (EU) 2018/1725 rendelettel (európai uniós adatvédelmi rendelet), mivel a személyes adatok védelmével kapcsolatos szempontok merülnek fel.

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos egyetért a javaslattal annak megállapítása tekintetében, hogy egy **MI-rendszer nagy kockázatú rendszerként** való besorolása **nem feltétlenül jelenti azt, hogy az** önmagában **jogszerű** és a felhasználó által alkalmazható. **Előfordulhat, hogy** az adatkezelőnek **az uniós adatvédelmi jogból eredő további követelményeknek is meg kell felelnie**. Ezen túlmenően az uniós (többek között a személyes adatok védelmére vonatkozó) jogszabályokból eredő jogi kötelezettségeknek való megfelelés előfeltétele kell, hogy legyen annak, hogy egy termék CE-jelöléssel ellátott termékként léphessen be az európai piacra. E célból az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy **az általános adatvédelmi rendeletnek és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletnek való megfelelés biztosítására vonatkozó követelményt bele kell foglalni a III. cím 2. fejezetébe**. Emellett az Európai Adatvédelmi Testület és az európai adatvédelmi biztos szükségesnek tartja a javaslatban foglalt megfelelőségértékelési eljárás kiigazítását annak érdekében, hogy harmadik felek minden esetben elvégezzék a nagy kockázatú MI-rendszerek előzetes megfelelőségértékelését.

A hátrányos megkülönböztetés nagy kockázatára tekintettel a javaslat tiltja a „közösségi pontozást” (social scoring) abban az esetben, ha arra „bizonyos időszakon keresztül”, illetve „hatóságok [által] vagy nevükben ” kerül sor. A magánvállalatok – például a közösségimédia- és felhőszolgáltatók – mindazonáltal szintén nagy mennyiségű személyes adatot kezelhetnek, és végezhetnek közösségi pontozást. Következésképpen **a jövőbeli MI-rendeletnek meg kell tiltania mindenfajta közösségi pontozást**.

Az egyének nyilvánosság számára hozzáférhető helyeken történő távoli biometrikus azonosítása az egyének magánéletébe való betolakodás nagy kockázatát hordozza magában, ami súlyos hatással van a lakosságnak a nyilvános helyeken való anonimitással kapcsolatos elvárásaira. Ezen okok miatt az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **szorgalmazza, hogy általános jelleggel tiltsák meg az MI-nek az emberi jellemzők** – például az arc, a járás, az ujjlenyomat, a DNS, a hang, a billentyűleütések és más biometrikus vagy viselkedési jellemzők – **alapján a nyilvánosság számára hozzáférhető helyeken történő automatikus felismerésre** bármilyen összefüggésben **történő használatát**. Szintén javasolt **betiltani azokat az MI-rendszereket, amelyek az egyéneket a biometrikus jellemzők alapján** etnikai hovatartozásuk, nemük, valamint politikai vagy szexuális irányultságuk vagy a hátrányos megkülönböztetésnek a Charta 21. cikke szerinti egyéb okai szerint **kategorizálják**. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli továbbá, hogy az MI **természetes személyek érzelmeinek levezetésére** való felhasználása **rendkívül nemkívánatos, és** azt **meg kell tiltani**.

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli **az európai adatvédelmi biztosnak az uniós intézmények, ügynökségek és szervek felügyeletére illetékes hatóságként és piacfelügyeleti hatóságként való kijelölését**. Az európai adatvédelmi biztos szerepét és feladatait azonban tovább kell pontosítani, különösen ami a piacfelügyeleti hatósági szerepét illeti. A jövőbeli MI-rendeletnek továbbá egyértelműen ki kell mondania, hogy **a felügyeleti hatóságok függetlenek** felügyeleti és végrehajtási feladataik ellátása során.

Az adatvédelmi hatóságok nemzeti felügyeleti hatóságként való kijelölése harmonizáltabb szabályozási megközelítést biztosítana, és hozzájárulna az adatkezelési rendelkezések következetesebb értelmezéséhez, valamint végrehajtásuk terén a tagállamok közötti ellentmondások elkerüléséhez. Következésképpen az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy **az adatvédelmi hatóságokat kell a javaslat 59. cikke alapján nemzeti felügyeleti hatóságként kijelölni**.

A javaslat meghatározó szerepet szán a Bizottságnak a Mesterséges Intelligenciával Foglalkozó Európai Testületben (EAIB). Ez a szerep ellentétes azzal, hogy a Mesterséges Intelligenciával Foglalkozó Európai Testületnek függetlennek kell lennie a politikai befolyástól. Függetlenségének garantálása érdekében a jövőbeli MI-rendeletnek **nagyobb autonómiát** kell biztosítania **az EAIB számára**, hogy saját kezdeményezésére cselekedhessen.

Figyelembe véve az MI-rendszerek egységes piacon való elterjedését és a határokon átnyúló esetek valószínűségét, elengedhetetlen a harmonizált végrehajtás és a hatáskörök megfelelő megosztása a nemzeti felügyeleti hatóságok között. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos olyan **mechanizmus** létrehozását javasolja, **amely minden egyes MI-rendszer esetében egyablakos ügyintézési pontot garantál a jogszabály által érintett egyének, valamint a vállalatok számára**.

Ami a **tesztkörnyezeteket** illeti, az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **javasolja azok hatályának és célkitűzéseinek pontosítását**. A javaslatnak egyértelműen ki kell mondania azt is, hogy az ilyen tesztkörnyezetek jogalapjának meg kell felelnie a hatályos adatvédelmi keretben meghatározott követelményeknek.

A javaslatban felvázolt **tanúsítási rendszer nem mutat egyértelmű kapcsolatot az uniós adatvédelmi joggal**, valamint a nagy kockázatú MI-rendszerek egyes „területeire” alkalmazandó egyéb uniós és tagállami jogszabályokkal, és nem veszi figyelembe **az adattakarékosság és a beépített adatvédelem elvét** mint **a CE-jelölés megszerzése előtt** figyelembe veendő szempontok egyikét. Ezért az Európai Adatvédelmi Testület és az európai adatvédelmi biztos javasolja a javaslat módosítását az említett rendelet alapján kiadott tanúsítványok és az adatvédelmi tanúsítványok, bélyegzők és jelölések közötti kapcsolat pontosítása érdekében. Végül az adatvédelmi hatóságokat be kell vonni a harmonizált szabványok és egységes előírások kidolgozásába és elfogadásába.

A **magatartási kódexeket** illetően az Európai Adatvédelmi Testület és az európai adatvédelmi biztos szerint **pontosítani szükséges**, hogy a személyes adatok védelmét az e magatartási kódexek által kezelhető „további követelmények” közé kell-e sorolni, és biztosítani kell, hogy a „műszaki előírások és megoldások” ne ütközzenek a hatályos uniós adatvédelmi keret szabályaiba és elveibe.

TARTALOMJEGYZÉK

Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos,

tekintettel a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről szóló, 2018. október 23-i (EU) 2018/1725 rendelet[1] 42. cikkének (2) bekezdésére,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére[2],

tekintettel az európai adatvédelmi biztosnak és az Európai Adatvédelmi Testületnek a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló rendeletre irányuló javaslatra vonatkozó közös véleményére irányuló 2021. április 22-i kérelemre,

A KÖVETKEZŐ KÖZÖS VÉLEMÉNYT FOGADTA EL

1 BEVEZETÉS

1. A mesterséges intelligencián (a továbbiakban: MI) alapuló rendszerek megjelenése nagyon fontos lépés a technológiák fejlődése és az emberek velük való érintkezésének módja terén. Az MI olyan kulcsfontosságú technológiák összessége, amelyek mind társadalmi, mind gazdasági szempontból alapjaiban változtatják meg mindennapi életünket. A következő néhány évben alapvető döntések várhatók az MI-vel kapcsolatban, mivel az segít leküzdeni a legnagyobb kihívások némelyikét, amelyekkel napjainkban számos területen szembesülünk az egészségügytől kezdve a mobilitáson át vagy a közigazgatástól az oktatásig.

2. Ezek az ígért előrelépések azonban kockázatokkal is járnak. A kockázatok nagyon is relevánsak, tekintve, hogy az MI-rendszerek egyéni és társadalmi hatásai nagyrészt még ismeretlenek. Az automatizált módon történő tartalomgenerálás, előrejelzés-készítés vagy döntéshozatal – ahogyan azt az MI-rendszerek teszik – gépi tanulási technikák vagy logikai és valószínűségi következtetési szabályok segítségével nem ugyanaz, mint amikor az emberek kreatív vagy elméleti érveléssel végzik ezeket a tevékenységeket, teljes felelősséget vállalva a következményekért.

3. Az adatok közötti mérhető – az emberi szem számára láthatatlan, de a gépek számára látható – összefüggésektől kezdve az MI számos területen bővíteni fogja az előrejelzések körét, megkönnyítve az életünket és megoldva számos problémát, de ugyanakkor aláássa azt a képességünket, hogy az eredményeket ok-okozati összefüggésben értelmezzük, oly módon, hogy az átláthatóság, az emberi ellenőrzés, az elszámoltathatóság és az eredményekért való felelősség fogalma komoly kihívásnak lesz kitéve.

[1] HL L 295., 2018.11.21., 39–98. o.

[2] A jelen dokumentumban a „tagállamokra" történő bármely hivatkozást „EGT-tagállamokra" történő hivatkozásként kell érteni.

4. A (személyes és nem személyes) adatok az MI-ben sok esetben az autonóm döntések kulcsfontosságú előfeltételei, ami elkerülhetetlenül hatással lesz az egyének életére különböző szinteken. Ezért az Európai Adatvédelmi Testület és az európai adatvédelmi biztos már ebben a szakaszban határozottan kijelenti, hogy a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló rendeletre irányuló javaslatnak (a továbbiakban: javaslat)[3] **fontos adatvédelmi vonatkozásai** vannak.

5. Az adatok alapján történő döntéshozatal feladatának gépekre való átruházása kockázatot jelent az egyének jogaira és szabadságaira, hatással lesz magánéletükre, és kárt okozhat csoportoknak vagy akár a társadalom egészének. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos hangsúlyozza, hogy a magánélethez és a személyes adatok védelméhez való jog, amellyel ellentétben áll az MI koncepciójának alapjául szolgáló gépi döntési autonómia feltételezése, az Emberi Jogok Egyetemes Nyilatkozatában (12. cikk), az Emberi Jogok Európai Egyezményében (8. cikk) és az Európai Unió Alapjogi Chartájában (a továbbiakban: Charta) (7. és 8. cikk) elismert uniós értékek egyik pillére. Az MI-alkalmazások által kínált növekedési perspektíva és az ember gépekkel szembeni központi szerepének és elsőbbségének összeegyeztetése nagyon ambiciózus, de szükséges cél.

6. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli az MI-értéklánc valamennyi érdekeltjének a szabályozásba való bevonását, valamint a megoldásszolgáltatókra vonatkozó egyedi követelmények bevezetését, mivel azok jelentős szerepet játszanak a rendszereiket felhasználó termékekben. A különböző felek – az MI-rendszer felhasználója, szolgáltatója, importőre vagy forgalmazója – felelősségi köreit azonban egyértelműen körül kell határolni és ki kell jelölni. Különösen a személyes adatok kezelése során különös figyelmet kell fordítani arra, hogy e szerepek és felelősségi körök összhangban legyenek az adatvédelmi keret szerinti adatkezelő és adatfeldolgozó fogalmával, mivel a két norma nem fedi egymást.

7. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli, hogy a javaslatban fontos helyet kap az emberi felügyelet fogalma (14. cikk). Ugyanakkor mivel egyes MI-rendszerek – a fent kifejtetteknek megfelelően – jelentős hatást gyakorolhatnak az egyénekre vagy egyének csoportjaira, a valódi emberközpontúságnak a magasan képzett személyek általi felügyeletre és a jogszerű adatkezelésre kell támaszkodnia, amennyiben az ilyen rendszerek személyes adatok kezelésén alapulnak, vagy feladataik ellátása érdekében személyes adatokat kezelnek, hogy biztosítva legyen, hogy tiszteletben tartják az érintett arra való jogosultságát, hogy ne terjedjen ki rá a kizárólag automatizált adatkezelésen alapuló döntés hatálya.

8. Emellett számos MI-alkalmazás adatintenzív jellege miatt a javaslatnak minden szinten elő kell mozdítania a beépített és alapértelmezett adatvédelemmel kapcsolatos megközelítés elfogadását, ösztönözve az adatvédelmi elvek hatékony végrehajtását (az általános adatvédelmi rendelet 25. cikkében és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 27. cikkében foglaltak szerint) a legkorszerűbb technológiák segítségével.

[3] COM(2021) 206 final.

9. Végezetül az Európai Adatvédelmi Testület és az európai adatvédelmi biztos hangsúlyozza, hogy ez a közös vélemény csak a javaslat előzetes elemzését tartalmazza, a javaslat hatásaira és az uniós adatvédelmi joggal való összeegyeztethetőségére vonatkozó további értékelés és vélemény sérelme nélkül.

2 A JAVASLAT ALAPELVEINEK ELEMZÉSE

2.1 A javaslat hatálya és a hatályos jogi kerettel való viszony

10. Az indokolás szerint a javaslat **jogalapja** elsősorban az EUMSZ 114. cikke, amely rendelkezik a belső piac létrehozását és működését biztosító intézkedések elfogadásáról[4]. Emellett a javaslat az EUMSZ 16. cikkén alapul, *amennyiben az a személyes adatok kezelése vonatkozásában az egyének védelmére vonatkozóan konkrét szabályokat tartalmaz*, nevezetesen korlátozza az MI-rendszerek használatát a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból történő „valós idejű" távoli biometrikus azonosítás terén[5].

11. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos emlékeztet arra, hogy az EUB ítélkezési gyakorlatával összhangban az EUMSZ 16. cikke megfelelő jogalapot biztosít akkor, ha a személyes adatok védelme képezi az uniós jogalkotó által elfogadott szabályok egyik célját vagy lényegi összetevőjét[6]. Az EUMSZ 16. cikkének alkalmazása azt is maga után vonja, hogy – amint azt a Charta 8. cikke is előírja – biztosítani kell a személyes adatok kezelésére vonatkozó követelmények tiszteletben tartásának független felügyeletét.

12. Az európai adatvédelmi biztos és az Európai Adatvédelmi Testület emlékeztet arra, hogy már létezik az EUMSZ 16. cikke alapján elfogadott átfogó adatvédelmi keretrendszer, amely az általános adatvédelmi rendeletből[7], az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletből (EUDPR)[8] és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvből[9] áll. A javaslat szerint csak a javaslatban szereplő, a biometrikus adatok kezelésére vonatkozó további korlátozások tekinthetők úgy, hogy azok az EUMSZ 16. cikkén alapulnak, és ezért ugyanazzal a jogalappal rendelkeznek, mint az általános adatvédelmi rendelet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet vagy a bűnüldözésben érvényesítendő

[4] Indokolás, 5. o.
[5] Indokolás, 6. o. Lásd a javaslat (2) preambulumbekezdését is.
[6] 2017. július 26-i vélemény, EU–Kanada PNR-megállapodás, 1/15, ECLI:EU:C:2017:592, 96. pont.
[7] 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 irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1–88. o.).
[8] Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39–98. o.).
[9] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89–131. o.).

adatvédelemről szóló irányelv. Ez általánosságban – a lent kifejtettek szerint – fontos következményekkel jár a javaslatnak az általános adatvédelmi rendelethez, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelethez, és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvhez fűződő viszonyára nézve.

13. **A javaslat hatályát** illetően az Európai Adatvédelmi Testület és az európai adatvédelmi biztos határozottan üdvözli, hogy a javaslat kiterjed az MI-rendszerek uniós intézmények, szervek vagy ügynökségek általi használatára. Tekintettel arra, hogy az MI-rendszerek e szervezetek általi használata – az uniós tagállamokban való felhasználáshoz hasonlóan – szintén jelentős hatással lehet az egyének alapvető jogaira, elengedhetetlen, hogy az MI-re vonatkozó új szabályozási keret mind az uniós tagállamokra, mind az uniós intézményekre, hivatalokra, szervekre és ügynökségekre alkalmazandó legyen az Unió-szerte koherens megközelítés biztosítása érdekében. Mivel az uniós intézmények, hivatalok, szervek és ügynökségek az MI-rendszerek szolgáltatóiként és felhasználóiként is felléphetnek, az európai adatvédelmi biztos és az Európai Adatvédelmi Testület teljes mértékben helyénvalónak tartja, hogy ezeket a szervezeteket az EUMSZ 114. cikke alapján a javaslat hatálya alá vonják.

14. Az Európai Adatvédelmi Testületnek és az európai adatvédelmi biztosnak mindazonáltal komoly aggályai vannak a nemzetközi bűnüldözési együttműködésnek a hatály alóli – a javaslat 2. cikkének (4) bekezdésében előírt – kizárásával kapcsolatban. Ez a kizárás a kijátszás jelentős kockázatával jár (például olyan harmadik országok vagy nemzetközi szervezetek, amelyek az EU-beli hatóságok által használt magas kockázatú alkalmazásokat működtetnek).

15. Az MI-rendszerek fejlesztése és használata sok esetben személyes adatok kezelésével jár. Rendkívül fontos annak biztosítása, hogy egyértelmű legyen e javaslatnak a hatályos uniós adatvédelmi szabályozással való viszonya. A javaslat nem sérti és kiegészíti az általános adatvédelmi rendeletet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet, és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet. Jóllehet a javaslat preambulumbekezdései egyértelművé teszik, hogy az MI-rendszerek használatának továbbra is meg kell felelnie az adatvédelmi jognak, **az Európai Adatvédelmi Testület és az európai adatvédelmi biztos határozottan javasolja annak pontosítását a javaslat 1. cikkében, hogy a személyes adatok védelmére vonatkozó uniós jogszabályokat** – különösen az általános adatvédelmi rendeletet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet, az elektronikus hírközlési adatvédelmi irányelvet[10] és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet – alkalmazni kell a személyes adatoknak a javaslat hatálya alá tartozó bármely kezelésére. Egy megfelelő preambulumbekezdésnek azt is pontosítania kell, hogy a javaslat nem szándékozik befolyásolni a személyes adatok kezelését szabályozó hatályos uniós jogszabályok alkalmazását, többek között az e jogi eszközöknek

[10] A 2006/24/EK irányelvvel és a 2009/136/EK irányelvvel módosított, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv („Elektronikus hírközlési adatvédelmi irányelv").

való megfelelés figyelemmel kísérésében illetékes független felügyeleti hatóságok feladatait és hatásköreit.

2.2 Kockázatalapú megközelítés

16. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **üdvözli** a javaslat alapjául szolgáló **kockázatalapú megközelítést**. A javaslat minden MI-rendszerre vonatkozna, ideértve azokat is, amelyek nem járnak személyes adatok kezelésével, de hatással lehetnek az érdekekre vagy az alapvető jogokra és szabadságokra.

17. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos megjegyzi, hogy a javaslat egyes rendelkezései figyelmen kívül hagyják az egyének csoportjait vagy a társadalom egészét érintő kockázatokat (például különös jelentőséggel bíró kollektív hatások, mint például csoportos hátrányos megkülönböztetés vagy politikai vélemények nyilvános helyeken történő kifejezése). Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt ajánlja, hogy az MI-rendszerek által jelentett társadalmi/csoportkockázatokat is fel kell mérni és mérsékelni kell.

18. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos véleménye szerint pontosítani kell a javaslat kockázatalapú megközelítését, az „alapvető jogokra jelentett kockázat" fogalmát pedig **összhangba kell hozni az általános adatvédelmi rendelettel**, amennyiben a személyes adatok védelmével kapcsolatos szempontok merülnek fel. Függetlenül attól, hogy végfelhasználókról, egyszerűen érintettekről vagy az MI-rendszer által érintett más személyekről van-e szó, a javaslat vakfoltjának tűnik, hogy a szöveg egyáltalán nem utal az MI-rendszer által érintett egyénre. Az érintett személyekkel szemben a szereplőkre rótt kötelezettségeknek konkrétabban az egyén és jogainak védelméből kell fakadniuk. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért szorgalmazza, hogy a jogalkotók kifejezetten foglalkozzanak a javaslatban az MI-rendszerek hatálya alá tartozó **egyének rendelkezésére álló jogokkal és jogorvoslatokkal**.

19. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos tudomásul veszi a **magas kockázatú MI-rendszerek** kimerítő jellegű listájának összeállítására vonatkozó döntést. Ez a döntés fekete-fehér hatást válthat ki a rendkívül kockázatos helyzetek gyenge vonzerejével, aláásva a javaslat alapjául szolgáló átfogó kockázatalapú megközelítést. Emellett a nagy kockázatú MI-rendszereknek a javaslat II. és III. mellékletében részletezett listája nem tartalmaz néhány olyan felhasználási esetet, amelyek jelentős kockázattal járnak, mint például MI használata a biztosítási díj meghatározásához, az orvosi kezelések értékeléséhez vagy az egészségügyi kutatáshoz. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt is kiemeli, hogy az említett mellékleteket rendszeresen frissíteni kellannak biztosítása érdekében, hogy hatályuk megfelelő legyen.

20. A javaslat előírja az MI-rendszer **szolgáltatói** számára, hogy végezzenek kockázatértékelést, a legtöbb esetben azonban az (adat)kezelők az MI-rendszerek **felhasználói**, nem pedig szolgáltatói lesznek (például az arcfelismerő rendszer felhasználója „adatkezelő", és ezért a javaslat alapján nem vonatkoznak rá a nagy kockázatú MI-szolgáltatókra vonatkozó követelmények).

21. Ezenfelül **a szolgáltatónak nem mindig lesz lehetősége értékelni** az MI-rendszer **valamennyi felhasználását**. Így a kezdeti kockázatértékelés általánosabb jellegű lesz, mint az MI-rendszer felhasználója által végzett értékelés. Még ha a szolgáltató által végzett kezdeti kockázatértékelés nem is utal arra, hogy az MI-rendszer „magas kockázatú" a javaslat értelmében, ez nem zárhatja ki a **későbbi (részletesebb) értékelést** (az általános adatvédelmi rendelet 35. cikke, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 39. cikke vagy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 27. cikke szerinti adatvédelmi hatásvizsgálatot), **amelyet a rendszer felhasználójának kell elvégeznie**, figyelembe véve a használat körülményeit és a konkrét felhasználási eseteket. Annak értékelését, hogy az általános adatvédelmi rendelet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv alapján az adatkezelés valamely típusa valószínűleg nagy kockázattal jár-e, a javaslattól függetlenül kell elvégezni. Valamely MI-rendszernek az alapvető jogokra gyakorolt hatása miatt[11] „nagy kockázatú" rendszerként való besorolása azonban **az általános adatvédelmi rendelet, európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet, és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv alapján a „nagy kockázat" vélelmét állítja fel, amennyiben személyes adatok feldolgozására kerül sor**.

22. **Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos egyetért a javaslattal annak megállapítása tekintetében, hogy egy MI-rendszer magas kockázatú rendszerként való besorolása nem feltétlenül jelenti azt, hogy az önmagában jogszerű és a felhasználó által alkalmazható. Előfordulhat, hogy az adatkezelőnek az uniós adatvédelmi jogból eredő további követelményeknek is meg kell felelnie.** Ezenkívül foglalkozni kell azzal a javaslat 5. cikkének alapjául szolgáló indokolással, amely szerint a tiltott rendszerekkel ellentétben a nagy kockázatú rendszerek főszabály szerint megengedhetők, és azt törölni kell a javaslatból, különösen mivel a javasolt CE-jelölés nem jelenti azt, hogy a személyes adatok kapcsolódó kezelése jogszerű.

23. Az uniós (többek között személyes adatok védelmére vonatkozó) jogszabályokból eredő jogi kötelezettségeknek való megfelelés mindazonáltal előfeltétele kell, hogy legyen annak, hogy egy termék CE-jelöléssel ellátott termékként léphessen be az európai piacra. E célból az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **azt ajánlja, hogy az általános adatvédelmi rendeletnek és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletnek való megfelelés biztosítására vonatkozó követelményt foglalják bele a javaslat III. címének 2. fejezetébe**. E követelményeket az elszámoltathatóság elvével összhangban (harmadik fél által végzett

[11] Az Európai Unió Alapjogi Ügynöksége (FRA) már foglalkozott azzal, hogy MI vagy kapcsolódó technológiák használata esetén alapjogi hatásvizsgálatot kell végezni. „[A helyes döntés – Mesterséges intelligencia és alapvető jogok (Getting the future right – Artificial intelligence and fundamental rights)]" című 2020. évi jelentésében az FRA „buktatókat azonosított az MI használatával kapcsolatban, például a prediktív rendészet, az orvosi diagnózisok, a szociális szolgáltatások és a célzott hirdetések terén", és hangsúlyozta, hogy az egyénekre gyakorolt negatív hatások csökkentése érdekében „a magán- és állami szervezeteknek értékelniük kell, hogy az MI hogyan sértheti az alapvető jogokat".

ellenőrzés útján) ellenőrizni kell a CE-jelölés előtt. E harmadik fél által végzett értékeléssel összefüggésben különösen fontos lesz a szolgáltató által elvégzendő kezdeti hatásvizsgálat.

24. Az MI-rendszerek fejlesztése által kiváltott összetettségre tekintettel rá kell mutatni arra, hogy az MI-rendszerek műszaki jellemzői (például az MI-megközelítés típusa) magasabb kockázattal járhatnak. Ezért az MI-rendszerek kockázatértékelése során minden esetben figyelembe kell venni **a műszaki jellemzőket a konkrét felhasználási esetekkel és a** rendszer működésének **körülményeivel** együtt.

25. A fentiek fényében az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt ajánlja, hogy a javaslatban pontosítsák, hogy a **szolgáltatónak** az érintett MI-rendszerre vonatkozó kezdeti kockázatértékelést kell végeznie, **figyelembe véve a felhasználási eseteket** (amelyeket a javaslatban kell meghatározni – kiegészítve például a III. melléklet 1. pontjának a) alpontját, amely nem említi a biometrikus MI-rendszerek felhasználási eseteit), valamint hogy az MI-rendszer **felhasználójának** az uniós adatvédelmi jog szerinti adatkezelői minőségében (adott esetben) adatvédelmi hatásvizsgálatot kell végeznie az általános adatvédelmi rendelet 35. cikkében, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 39. cikkében és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 27. cikkében foglaltaknak megfelelően, figyelembe véve nemcsak a műszaki jellemzőket és a **felhasználási eseteket**, hanem az MI jövőbeli működésének **konkrét körülményeit is**.

26. Ezenkívül pontosítani kell a javaslat III. mellékletében említett kifejezések némelyikét, például az „alapvető magánszolgáltatások” kifejezést vagy a hitelképességi vizsgálat során MI-t saját célra használó kis szolgáltató fogalmát.

2.3 Az MI tiltott felhasználásai

27. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy **az MI tolakodó formáit** – különösen azokat, amelyek sérthetik az emberi méltóságot – a javaslat 5. cikke értelmében tiltott MI-rendszereknek kell tekinteni ahelyett, hogy egyszerűen „magas kockázatúnak” minősítenék őket a javaslat III. mellékletében, mint például a 6. pontban szereplőket. Ez különösen azokra az adat-összehasonlításokra vonatkozik, amelyek nagymértékben olyan személyeket is érintenek, akik nem vagy csak csekély mértékben adtak okot a rendőrségi megfigyelésre, vagy az olyan adatkezelésre, amely sérti az adatvédelmi jog szerinti célhoz kötöttség elvét. Az MI rendőrségi és bűnüldözési célú használatához területspecifikus, pontos, előrelátható és arányos szabályokra van szükség, amelyeknek figyelembe kell venniük az érintett személyek érdekeit és a demokratikus társadalom működésére gyakorolt hatásokat.

28. A javaslat 5. cikke azzal a kockázattal jár, hogy az „értékek” és az azokkal ellentétes MI-rendszerek tilalma csak a szavak szintjén jelenik meg. Az 5. cikkben említett, az MI-rendszerek tiltottnak „minősítésére” vonatkozó kritériumok ugyanis olyan mértékben **korlátozzák a tilalom hatályát**, hogy az a gyakorlatban értelmetlenné válhat (például „testi vagy lelki károsodást okoz vagy okozhat” az 5. cikk (1) bekezdésének a) és b) pontjában; a hatóságokra való korlátozás az 5. cikk (1) bekezdésének c) pontjában; homályos megfogalmazás a c) pont

i. és ii. alpontjában; a „valós idejű” távoli biometrikus azonosításra való korlátozás egyértelmű fogalommeghatározás nélkül stb.).

29. Különösen az MI – a javaslat 5. cikke (1) bekezdésének c) pontja szerinti – „közösségi pontozásra” való használata hátrányos megkülönböztetéshez vezethet, és ellentétes az EU alapvető értékeivel. A javaslat csak abban az esetben tiltja ezeket a gyakorlatokat, ha azokat „bizonyos időszakon keresztül”, illetve „hatóságok által vagy nevükben” alkalmazzák. A magánvállalatok – különösen a közösségimédia- és felhőszolgáltatók – nagy mennyiségű személyes adatot kezelhetnek, és végezhetnek közösségi pontozást. Következésképpen **a javaslatnak meg kell tiltania mindenfajta közösségi pontozást**. Meg kell jegyezni, hogy a bűnüldözéssel összefüggésben a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv 4. cikke már jelentős mértékben korlátozza – ha a gyakorlatban nem is tiltja – az ilyen típusú tevékenységeket.

30. Az egyének nyilvánosság számára hozzáférhető helyeken történő **távoli biometrikus azonosítása** az egyének magánéletébe való betolakodás magas kockázatát hordozza magában. Ezért az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **úgy véli, hogy szigorúbb megközelítésre van szükség**. Az MI-rendszerek használata súlyos arányossági problémákat vethet fel, mivel válogatás nélküli és aránytalan számú érintett adatainak kezelésével járhat csupán néhány egyén azonosítása céljából (például a repülőtereken és vasútállomásokon tartózkodó utasok). A távoli biometrikus azonosítási rendszerek **zökkenőmentes** jellege átláthatósági problémákat és az uniós jog (a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv, az általános adatvédelmi rendelet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet és más alkalmazandó jogszabályok) szerinti adatkezelés jogalapjával kapcsolatos kérdéseket is felvet. Az egyének ezen adatkezelésről való megfelelő tájékoztatásának módjával, valamint az egyének jogainak hatékony és időben történő gyakorlásával kapcsolatos probléma továbbra is megoldatlan. Ugyanez vonatkozik a távoli biometrikus azonosítás által **a lakosságnak a nyilvános helyeken való anonimitással kapcsolatos** (észszerű) **elvárásaira gyakorolt visszafordíthatatlan és súlyos hatásra** is, ami közvetlen negatív hatást gyakorol a véleménynyilvánítás, a gyülekezés, az egyesülés és a mozgás szabadságának gyakorlására.

31. A javaslat 5. cikke (1) bekezdésének d) pontja kimerítően **felsorolja azokat a kivételes eseteket**, amelyekben bűnüldözési célokból megengedett a nyilvánosság számára hozzáférhető helyeken a „valós idejű” távoli biometrikus azonosítás. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy **ez a megközelítés** több szempontból is **hibás**: először is nem világos, hogy mit kell „jelentős késleltetés” alatt érteni, és hogyan kell azt enyhítő tényezőnek tekinteni, figyelembe véve, hogy egy tömeges azonosítási rendszer csupán néhány órán belül több ezer egyént képes azonosítani. Ezenkívül az adatkezelés tolakodó jellege nem mindig függ attól, hogy az azonosításra valós időben kerül-e sor vagy sem. A nem valós idejű távoli biometrikus azonosítás egy politikai tiltakozással összefüggésben valószínűleg jelentős visszatartó hatással lesz az olyan alapvető jogok és szabadságok gyakorlására, mint a gyülekezési és egyesülési szabadság, valamint általánosabban a demokrácia alapelvei. Másodszor, az adatkezelés tolakodó jellege nem feltétlenül függ az adatkezelés céljától. E rendszer más célokra, például személy- és vagyonvédelemre való

használata ugyanolyan veszélyt jelent a magán- és a családi élet tiszteletben tartásához és a személyes adatok védelméhez való alapvető jogra nézve. Végül, még a tervezett korlátozások mellett is, a bűncselekmények gyanúsítottjainak vagy elkövetőinek potenciális száma szinte mindig „kellően magas” lesz ahhoz, hogy a javaslat 5. cikkének (2)–(4) bekezdésében foglalt további feltételek ellenére indokolttá tegye az MI-rendszereknek a gyanúsítottak felderítésére való folyamatos használatát. Úgy tűnik, hogy a javaslat indoklása figyelmen kívül hagyja, hogy a nyílt területek megfigyelése során az uniós adatvédelmi jog szerinti kötelezettségeket nemcsak a gyanúsítottak, hanem mindazok esetében be kell tartani, akiket a gyakorlatban megfigyelnek.

32. Mindezen okok miatt az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **szorgalmazza, hogy általános jelleggel tiltsák meg az MI-nek az emberi jellemzők – például az arc, a járás, az ujjlenyomat, a DNS, a hang, a billentyűleütések és más biometrikus vagy viselkedési jellemzők – alapján a nyilvánosság számára hozzáférhető helyeken történő automatikus felismerésre bármilyen összefüggésben történő használatát**. A javaslat jelenlegi megközelítése az összes betiltandó MI-rendszer azonosítása és felsorolása. A következetesség érdekében tehát a javaslat 5. cikkében be kell tiltani **az online terekben nagymérvű távoli azonosításra szolgáló MI-rendszereket**. Figyelembe véve a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet és az általános adatvédelmi rendeletet, az európai adatvédelmi biztos és az Európai Adatvédelmi Testület nem látja, hogy ez a fajta gyakorlat hogyan felelne meg a szükségesség és arányosság követelményének, és ez végső soron abból következik, amit az EUB és az EJEB az alapvető jogokba való elfogadható beavatkozásnak tekint.

33. Ezenfelül az Európai Adatvédelmi Testület és az európai adatvédelmi biztos **azt ajánlja, hogy** mind a hatóságok, mind a magánszervezetek számára **tiltsák be azokat az MI-rendszereket, amelyek az egyéneket a biometrikus jellemzők (például arcfelismerés) alapján etnikai hovatartozásuk, nemük, valamint politikai vagy szexuális irányultságuk vagy a hátrányos megkülönböztetésnek a Charta 21. cikke által tiltott egyéb okai szerint kategorizálják, vagy** azokat az MI-rendszereket, amelyek tudományos megalapozottsága nem bizonyított, vagy amelyek közvetlen ellentétben állnak az EU alapvető értékeivel (például poligráf, a III. melléklet 6. pontjának b) alpontja és 7. pontjának a) alpontja). Ennek megfelelően **az 5. cikkben meg kell tiltani a „biometrikus kategorizálást”**.

34. **Az emberi méltóságot** is **sérti, ha egy számítógép a saját szabad akaratától függetlenül meghatározza vagy besorolja az ember jövőbeli viselkedését**. Az olyan MI-rendszerek, amelyeket a bűnüldöző hatóságok a természetes személyekre vonatkozó egyedi kockázatértékelések elvégzésére használnak annak értékelése céljából, hogy egy természetes személy milyen kockázatot jelenthet a bűncselekmény elkövetése vagy újbóli elkövetése szempontjából (lásd a III. melléklet 6. pontjának a) alpontját), vagy az olyan MI-rendszerek rendeltetésszerű használata, amelyeket a bűnüldöző hatóságok a természetes személyekre vonatkozó profilalkotás alapján vagy a személyiségbeli jellemzők és tulajdonságok vagy múltbeli bűnöző magatartás értékelése alapján tényleges vagy potenciális bűncselekmények előfordulásának vagy megismétlődésének előrejelzésére használnak (lásd a III. melléklet 6.

pontjának e) alpontját), a rendőri és igazságügyi döntéshozatal alapvető alávetettségéhez vezet, tárgyiasítva ezáltal az érintett embert. Az 5. cikkben be kell tiltani az ilyen, az emberi méltósághoz való jog lényegét érintő MI-rendszereket.

35. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli továbbá, hogy az MI **természetes személyek érzelmeinek levezetésére** való felhasználása **rendkívül nemkívánatos, és azt meg kell tiltani** bizonyos jól meghatározott felhasználási esetek – nevezetesen az egészségügyi vagy kutatási célú felhasználás (például betegek, akiknek esetében fontos az érzelmek felismerése) – kivételével, minden esetben megfelelő biztosítékok és természetesen az összes többi adatvédelmi feltétel és korlátozás alkalmazása mellett, ideértve a célhoz kötöttséget is.

2.4 Magas kockázatú MI-rendszerek

2.4.1 A külső harmadik felek általi előzetes megfelelőségértékelés szükségessége

36. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli, hogy a magas kockázatot jelentő MI-rendszereket előzetes megfelelőségértékelés alá kell vetni azok EU-beli forgalomba hozatala vagy más módon történő üzembe helyezése előtt. Ez a szabályozási modell elvben üdvözlendő, mivel megfelelő egyensúlyt teremt az innováció elősegítése és az alapvető jogok magas szintű proaktív védelme között. Ahhoz, hogy meghatározott környezetben, például a közintézmények döntéshozatali eljárásaiban vagy a kritikus infrastruktúrákban alkalmazni lehessen őket, meg kell határozni a teljes forráskód megvizsgálásának módjait.

37. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azonban a javaslat 43. cikke szerinti megfelelőségértékelési eljárás kiigazítását javasolja annak érdekében, hogy **a magas kockázatú MI esetében általában harmadik fél által végzett előzetes megfelelőségértékelésre kerüljön sor**. Bár az általános adatvédelmi rendelet vagy az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet nem követeli meg a személyes adatok nagy kockázatú kezelésének harmadik fél által végzett megfelelőségértékelését, az MI-rendszerek által jelentett kockázatokat még teljes mértékben meg kell érteni. A harmadik fél által végzett megfelelőségértékelésre vonatkozó kötelezettség általános bevezetése ezért tovább erősítené a jogbiztonságot és a nagy kockázatú MI-rendszerek iránti bizalmat.

2.4.2 A szabályozás hatályának a már használatban lévő MI-rendszerekre is ki kell terjednie

38. A javaslat 43. cikkének (4) bekezdése értelmében a magas kockázatú MI-rendszereket új megfelelőségértékelési eljárásnak kell alávetni akkor, amikor lényeges módosításra kerül sor. Helyes annak biztosítása, hogy az MI-rendszerek teljes életciklusuk során megfeleljenek az MI-rendelet követelményeinek. Azok az MI-rendszerek, amelyeket a javasolt rendelet alkalmazása előtt (vagy a IX. mellékletben felsorolt nagyméretű informatikai rendszerek esetében 12 hónappal azt követően) hoztak forgalomba vagy helyeztek üzembe, ki vannak zárva a rendelet hatálya alól, kivéve, ha a szóban forgó rendszerek kialakításukban vagy rendeltetésükben „jelentős változásokon” mennek keresztül (83. cikk).

39. Nem egyértelmű azonban a „jelentős változások” küszöbértéke. A javaslat (66) preambulumbekezdése alacsonyabb küszöbértéket határoz meg a megfelelőség újraértékelése tekintetében, „valahányszor olyan változás következik be, amely befolyásolhatja a megfelelést”. Hasonló küszöbérték lenne megfelelő a 83. cikk esetében is, legalábbis a nagy kockázatú MI-rendszerek tekintetében. Ezenkívül a védelmi hiányosságok megszüntetése érdekében a már létrehozott és működő MI-rendszereknek – egy bizonyos végrehajtási időszakot követően – szintén meg kell felelniük az MI-rendelet valamennyi követelményének.

40. A személyes adatok kezelésének sokrétű lehetőségei és a külső kockázatok szintén hatással vannak az MI-rendszerek biztonságára. A 83. cikknek a „tervezés[…] vagy rendeltetés[…] jelentős megváltozásá[ra]” helyezett hangsúlya nem hivatkozik a külső kockázatok megváltozására. Ezért a javaslat 83. cikkében hivatkozni kell a fenyegetési forgatókönyvek külső kockázatokból – például kibertámadásokból, ellenséges támadásokból és megalapozott fogyasztói panaszokból – eredő változásaira.

41. Továbbá, mivel az alkalmazás a jövőbeli rendelet hatálybalépésétől számított 24 hónap elteltével kezdődik, az európai adatvédelmi biztos és az Európai Adatvédelmi Testület nem tartja helyénvalónak, hogy a korábban már forgalomba hozott MI-rendszereket még hosszabb időre mentesítsék. Jóllehet a javaslat azt is előírja, hogy a rendelet követelményeit figyelembe kell venni minden egyes, a IX. mellékletben felsorolt jogi aktusokkal létrehozott nagyméretű informatikai rendszer értékelése során, az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy az MI-rendszerek üzembe helyezésére és használatára vonatkozó követelményeket a jövőbeli rendelet alkalmazásának kezdőnapjától kell alkalmazni.

2.5 Irányítás és a Mesterséges Intelligenciával Foglalkozó Európai Testület

2.5.1 Irányítás

42. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli az európai adatvédelmi biztosnak az uniós intézmények, ügynökségek és szervek felügyeletére illetékes hatóságként és piacfelügyeleti hatóságként való kijelölését, ha azok e javaslat hatálya alá tartoznak. Az európai adatvédelmi biztos készen áll arra, hogy betöltse az uniós közigazgatás MI-vel foglalkozó szabályozójának új szerepét. Az európai adatvédelmi biztos szerepe és feladatai ezenfelül nincsenek kellőképpen részletezve, és azokat tovább kell pontosítani a javaslatban, különösen ami a piacfelügyeleti hatósági szerepét illeti.

43. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos tudomásul veszi a javaslat által a Testület és a bejelentő szervként eljáró európai adatvédelmi biztos számára előirányzott pénzügyi források elosztását. Az európai adatvédelmi biztos számára előírt új feladatok teljesítéséhez azonban – függetlenül attól, hogy bejelentett szervezetként jár-e el – lényegesen több pénzügyi és emberi erőforrásra lenne szükség.

44. Először is, mivel a 63. cikk (6) bekezdésének szövege kimondja, hogy az európai adatvédelmi biztos „piacfelügyeleti hatóságként jár el” a javaslat hatálya alá tartozó uniós intézmények, ügynökségek és szervek tekintetében, ami nem tisztázza, hogy az európai adatvédelmi biztost teljes mértékben az (EU) 2019/1020 rendelet szerinti „piacfelügyeleti hatóságnak” kell-e tekinteni. Ez kérdéseket vet fel az európai adatvédelmi biztos gyakorlati feladataival és

hatásköreivel kapcsolatban. Másodszor, és feltéve, hogy az előző kérdésre igenlő választ kell adni, nem egyértelmű, hogy az európai adatvédelmi biztosnak az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletben meghatározott szerepe hogyan egyeztethető össze az (EU) 2019/1020 rendelet 11. cikkében előírt feladattal, amely „a területükön belül a hatékony piacfelügyelet az online […] forgalmazott […] termékek tekintetében” vagy „a megfelelő mintákon alapuló fizikai és laboratóriumi ellenőrzések” feladatát foglalja magában. Fennáll a kockázata annak, hogy az új feladatoknak a javaslatban elvégzett további pontosítások nélküli ellátása veszélyeztetheti az adatvédelmi biztosként rá háruló kötelezettségek teljesítését.

45. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos mindazonáltal hangsúlyozza, hogy a javaslat egyes rendelkezései, amelyek meghatározzák az MI-rendelet szerinti különböző illetékes hatóságok feladatait és hatásköreit, egymás közötti viszonyukat, jellegüket és függetlenségük garanciáit, nem tűnnek egyértelműnek ebben a szakaszban. Míg az (EU) 2019/1020 rendelet kimondja, hogy a piacfelügyeleti hatóságnak függetlennek kell lennie, a rendelettervezet nem írja elő a felügyeleti hatóságok függetlenségét, sőt azt írja elő számukra, hogy tegyenek jelentést a Bizottságnak a piacfelügyeleti hatóságok által végzett bizonyos feladatokról, amelyek különböző intézmények lehetnek. Mivel a javaslat azt is kimondja, hogy az adatvédelmi hatóságok lesznek a piacfelügyeleti hatóságok a bűnüldözési célokra használt MI-rendszerek esetében (a 63. cikk (5) bekezdése), ez azt is jelenti, hogy – esetlegesen a nemzeti felügyeleti hatóságukon keresztül – a Bizottsággal szemben fennálló jelentéstételi kötelezettség hatálya alá tartoznak majd (a 63. cikk (2) bekezdése), ami összeegyeztethetetlennek tűnik függetlenségükkel.

46. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért úgy véli, hogy ezeket a rendelkezéseket pontosítani kell a 2019/1020 rendelettel, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelettel és az általános adatvédelmi rendelettel való összhang megteremtése érdekében, és a javaslatnak egyértelműen ki kell mondania, hogy az MI-rendelet szerinti felügyeleti hatóságoknak teljes mértékben függetlennek kell lenniük feladataik ellátása során, mivel ez a jövőbeli rendelet megfelelő felügyeletének és végrehajtásának alapvető garanciája lenne.

47. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos arra is szeretne emlékeztetni, hogy az adatvédelmi hatóságok a személyes adatokat tartalmazó MI-rendszerek vonatkozásában már most is érvényesítik az általános adatvédelmi rendeletet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet az alapvető jogok és különösen az adatvédelemhez való jog védelmének biztosítása érdekében. Ezért az adatvédelmi hatóságok – amint azt a javaslat a nemzeti felügyeleti hatóságok tekintetében megköveteli – már rendelkeznek az MI-technológiákra, az adatokra, az adatfeldolgozásra és az alapvető jogokra vonatkozó bizonyos fokú ismeretekkel, valamint az új technológiák által az alapvető jogokra jelentett kockázatok értékelésére vonatkozó szakértelemmel. Ezenkívül amennyiben az MI-rendszerek személyes adatok kezelésén alapulnak vagy személyes adatokat kezelnek, a javaslat rendelkezései közvetlenül összefonódnak az adatvédelmi jogi kerettel, a rendelet hatálya alá tartozó MI-rendszerek többsége esetében pedig ez lesz a helyzet. Ennek

eredményeként össze fognak kapcsolódni a hatáskörök a javaslat szerinti felügyeleti hatóságok és az adatvédelmi hatóságok között.

48. Ebből következően az adatvédelmi hatóságok nemzeti felügyeleti hatóságként való kijelölése harmonizáltabb szabályozási megközelítést biztosítana, és hozzájárulna az adatkezelési rendelkezések következetesebb értelmezéséhez, valamint végrehajtásuk terén a tagállamok közötti ellentmondások elkerüléséhez. Az MI-értéklánc valamennyi érdekeltje számára is előnyös lenne, ha a javaslat hatálya alá tartozó valamennyi személyesadat-kezelési művelet tekintetében egyetlen egyablakos ügyintézési pont állna rendelkezésre, és korlátozódna a javaslat és az általános adatvédelmi rendelet által érintett két különböző adatkezelési szabályozó szerv közötti kapcsolattartás. Következésképpen az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy **az adatvédelmi hatóságokat kell a javaslat 59. cikke alapján nemzeti felügyeleti hatóságként kijelölni**.

49. Mindenesetre, amennyiben a javaslat a személyes adatok kezelése vonatkozásában az egyének védelmére vonatkozóan az EUMSZ 16. cikke alapján elfogadott konkrét szabályokat tartalmaz, az e szabályoknak való megfelelést – nevezetesen az MI-rendszereknek a nyilvánosság számára hozzáférhető helyeken, bűnüldözés céljából „valós idejű” távoli biometrikus azonosításra történő használatát érintő korlátozásokat – **független hatóságoknak kell ellenőrizniük**.

50. A javaslat azonban nem tartalmaz olyan kifejezett rendelkezést, amely az e szabályoknak való megfelelés biztosítására vonatkozó hatáskört független hatóságokra ruházná. Az általános adatvédelmi rendelet vagy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv szerinti illetékes adatvédelmi felügyeleti hatóságokra csak a javaslat 63. cikkének (5) bekezdése hivatkozik, de csak „piacfelügyeleti” szervként, illetve néhány más hatósággal együtt. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli, hogy ez a rendszer nem biztosítja az EUMSZ 16. cikkének (2) bekezdésében és a Charta 8. cikkében meghatározott független ellenőrzés követelményének való megfelelést.

2.5.2 A Mesterséges Intelligenciával Foglalkozó Európai Testület

51. A javaslat létrehozza a „Mesterséges Intelligenciával Foglalkozó Európai Testületet” (EAIB). Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos elismeri a javasolt keret következetes és harmonizált alkalmazásának szükségességét, valamint azt, hogy független szakértőket kell bevonni az MI-vel kapcsolatos uniós szakpolitika kidolgozásába. A javaslat ugyanakkor meghatározó szerepet irányoz elő a Bizottság számára. A Bizottság ugyanis nemcsak az EAIB tagja lenne, hanem annak elnöki tisztét is betöltené, és vétójoggal rendelkezne az EAIB eljárási szabályzatának elfogadását illetően. Ez ellentétben áll azzal, hogy a Mesterséges Intelligenciával Foglalkozó Európai Testületnek függetlennek kell lennie a politikai befolyástól. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért úgy véli, hogy a jövőbeli MI-rendeletnek **nagyobb autonómiát** kell biztosítania **az EAIB számára** annak érdekében, hogy az valóban biztosíthassa a rendelet egységes piacon belüli következetes alkalmazását.

52. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt is megjegyzi, hogy az EAIB nem kap hatáskört a javasolt rendelet végrehajtására. Figyelembe véve azonban az MI-rendszerek egységes piacon való elterjedését és a határokon átnyúló esetek valószínűségét, elengedhetetlen a harmonizált végrehajtás és a hatáskörök megfelelő megosztása a nemzeti felügyeleti hatóságok között. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért azt ajánlja, hogy a jövőbeli MI-rendeletben határozzák meg a nemzeti felügyeleti hatóságok közötti együttműködési mechanizmusokat. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos olyan mechanizmus bevezetését javasolja, amely minden egyes MI-rendszer esetében egyablakos ügyintézési pontot garantál a jogszabály által érintett egyének, valamint a vállalatok számára, valamint hogy azon szervezetek esetében, amelyek tevékenysége az uniós tagállamok több mint felét lefedi, az EAIB kijelölhesse azt a nemzeti hatóságot, amely felelős lesz az MI-rendeletnek az adott MI-rendszer tekintetében történő végrehajtásáért.

53. Továbbá, figyelembe véve a Testületet alkotó hatóságok független jellegét, a Testületet fel kell jogosítani arra, hogy saját kezdeményezésére cselekedjen, és ne csak tanácsot és segítséget nyújtson a Bizottságnak. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért hangsúlyozza, hogy ki kell terjeszteni a Testület feladatkörét, amely emellett nem egyezik meg a javaslatban felsorolt feladatokkal.

54. E célok elérése érdekében **az EAIB-nek elegendő és megfelelő hatáskörrel kell rendelkeznie**, jogállását pedig pontosítani kell. Különösen ahhoz, hogy a jövőbeli rendelet tárgyi hatálya továbbra is releváns maradjon, úgy tűnik, hogy az alkalmazásáért felelős hatóságokat be kell vonni annak kidolgozásába. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért azt javasolja, hogy az EAIB kapjon felhatalmazást arra, hogy javaslatot tegyen a Bizottságnak az MI-vel kapcsolatos technikákat és megközelítéseket meghatározó I. melléklet, valamint a 6. cikk (2) bekezdése értelmében vett nagy kockázatú MI-rendszereket felsoroló III. melléklet módosítására. A Bizottságnak emellett konzultálnia kellene az EAIB-vel, mielőtt módosítaná ezeket a mellékleteket.

55. A javaslat 57. cikkének (4) bekezdése információcserét ír elő a Testület és más uniós szervek, hivatalok, ügynökségek és tanácsadó csoportok között. Figyelembe véve az MI területén végzett korábbi munkáját és emberi jogi szakértelmét, az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt javasolja, hogy az Alapjogi Ügynökséget vegyék fontolóra a Testület egyik megfigyelőjeként.

3 AZ ADATVÉDELMI KERETTEL VALÓ KÖLCSÖNHATÁS

3.1 A javaslatnak a hatályos uniós adatvédelmi joggal való viszonya

56. A javaslat és a hatályos adatvédelmi jog közötti egyértelműen meghatározott viszony alapvető előfeltétele a személyes adatok védelmére vonatkozó uniós vívmányok tiszteletben tartása és alkalmazása biztosításának és fenntartásának. Az ilyen uniós jogot – különösen az általános adatvédelmi rendeletet, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet és a bűnüldözésben érvényesítendő

adatvédelemről szóló irányelvet – olyan előfeltételnek kell tekinteni, amelyre további jogalkotási javaslatok épülhetnek anélkül, hogy érintenék a hatályos rendelkezéseket, vagy összeütközésbe kerülnének azokkal, ideértve a felügyeleti hatóságok hatáskörét és a kormányzást is.

57. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos véleménye szerint ezért a javaslatban egyértelműen el kell kerülni az általános adatvédelmi rendelettel, az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelettel és a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel való összeegyeztethetetlenséget és esetleges összeütközést. Ez nemcsak a jogbiztonság, hanem annak elkerülése érdekében is szükséges, hogy a javaslat közvetlen vagy közvetett módon veszélyeztesse az EUMSZ 16. cikkében és a Charta 8. cikkében rögzített személyes adatok védelméhez való alapvető jogot.

58. Öntanuló gépek különösen csak akkor védhetik meg az egyének személyes adatait, ha ez a koncepció részeként eleve be van építve. Szintén alapvető fontosságú az egyéneknek az általános adatvédelmi rendelet 22. cikke (automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást) vagy az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 23. cikke szerinti jogai gyakorlásának azonnali lehetősége az adatkezelés céljától függetlenül. E tekintetben az MI-rendszerekben kezdettől fogva biztosítani kell az érintetteknek az adatvédelmi jogszabályok szerinti – a törléshez és helyesbítéshez való joggal kapcsolatos – jogait a választott MI-megközelítéstől vagy a műszaki architektúrától függetlenül.

59. Személyes adatoknak az MI-rendszerek tanulásához való felhasználása torzult döntéshozatali minták kialakulásához vezethet az MI-rendszer középpontjában. Az ilyen folyamatokban ezért különböző biztosítékokat és különösen képzett személyek általi felügyeletet kell előírni az érintettek jogai tiszteletben tartásának és garantálásának biztosítása, valamint az egyénekre gyakorolt bármely és minden negatív hatás elkerülése érdekében. Az illetékes hatóságok számára lehetővé kell tenni, hogy iránymutatásokat javasoljanak az MI-rendszerek torzulásának értékelésére és az emberi felügyelet gyakorlásának támogatására.

60. Az érintetteket minden esetben tájékoztatni kell arról, ha adataikat MI-betanításra és/vagy -előrejelzésre használják fel, az ilyen adatkezelés jogalapjáról, valamint az MI-rendszer logikájának (eljárásának) és hatályának általános magyarázatáról. E tekintetben ezekben az esetekben mindig biztosítani kell az egyéneknek az adatkezelés korlátozásához (az általános adatvédelmi rendelet 18. cikke és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 20. cikke), valamint az adatok törléséhez (az általános adatvédelmi rendelet 16. cikke és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 19. cikke) való jogát. Az adatkezelőt továbbá kifejezetten kötelezni kell arra, hogy tájékoztassa az érintettet a kifogásolásra, a korlátozásra, az adatok törlésére stb. vonatkozó határidőkről. Az MI-rendszernek képesnek kell lennie arra, hogy megfelelő technikai és szervezeti intézkedések révén megfeleljen az összes adatvédelmi követelménynek. A magyarázathoz való jognak fokozottabb átláthatóságot kell biztosítania.

3.2 Tesztkörnyezet és további adatkezelés (a javaslat 53. és 54. cikke)

61. A fennálló jogi és erkölcsi korlátokon belül fontos az európai innováció támogatása olyan eszközök révén, mint például egy tesztkörnyezet. A tesztkörnyezet lehetőséget ad az MI-rendszerek iránti bizalom kiépítéséhez szükséges biztosítékok megteremtésére. Összetett környezetben nehézséget okozhat az MI-vel foglalkozó szakemberek számára, hogy minden érdeket megfelelően mérlegeljenek. Különösen a korlátozott erőforrásokkal rendelkező kis- és középvállalkozások esetében a szabályozói tesztkörnyezetben való működés gyorsabb betekintést nyújthat, és ezáltal előmozdíthatja az innovációt.

62. A javaslat 53. cikkének (3) bekezdése értelmében a tesztkörnyezet nem érinti a felügyeleti és korrekciós hatásköröket. Ha ez a pontosítás hasznos, akkor szintén útmutatást vagy iránymutatást kell adni arra vonatkozóan, hogy miként lehet megfelelő egyensúlyt teremteni egyrészt a felügyeleti hatóságként való eljárás, másrészt részletes iránymutatásnak egy tesztkörnyezet révén történő nyújtása között.

63. Az 53. cikk (6) bekezdése előírja, hogy a tesztkörnyezetek működésének módozatait és feltételeit végrehajtási jogi aktusokban kell meghatározni. Fontos, hogy konkrét iránymutatások készüljenek, biztosítandó a tesztkörnyezetek létrehozásának és működtetésének egységességét és támogatását. A kötelező erejű végrehajtási jogi aktusok azonban korlátozhatják az egyes tagállamok arra való képességét, hogy szükségleteiknek és helyi gyakorlataiknak megfelelően testre szabják a tesztkörnyezetet. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért azt javasolja, hogy az EAIB adjon iránymutatást a tesztkörnyezetekre vonatkozóan.

64. A javaslat 54. cikke jogalapot kíván biztosítani a személyes adatok bizonyos közérdekű MI-rendszerek fejlesztése céljából az MI-re vonatkozó szabályozói tesztkörnyezetben történő további kezeléséhez. A javaslat 54. cikke (1) bekezdésének a javaslat 54. cikkének (2) bekezdéséhez és (41) preambulumbekezdéséhez és így a hatályos uniós adatvédelmi joghoz fűződő viszonya nem egyértelmű. Az általános adatvédelmi rendelet és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet azonban már tartalmaz a „további adatkezelésre" vonatkozó jogalapot. Különösen azokban az esetekben, amelyekben a további adatkezelés engedélyezése közérdek, az adatkezelő érdekei és az érintett érdekei közötti egyensúly megteremtésének nem kell akadályoznia az innovációt. A javaslat 54. cikke jelenleg nem foglalkozik két fontos kérdéssel: i. milyen körülmények között, milyen (további) kritériumok alapján kell mérlegelni az érintettek érdekeit, és ii. ezeket az MI-rendszereket csak a tesztkörnyezetben fogják-e használni. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli azt a követelményt, hogy a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv alapján gyűjtött személyes adatok tesztkörnyezetben történő kezelése során uniós vagy tagállami jogszabályra van szükség, de azt ajánlja, hogy az általános adatvédelmi rendelettel és európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelettel összhangban álló módon pontosítsák tovább a javaslat szóban forgó rendelkezését, elsősorban annak pontosításával, hogy az ilyen tesztkörnyezetek jogalapjának meg kell felelnie az általános adatvédelmi rendelet 23. cikkének (2) bekezdésében és az európai uniós intézményekre,

hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet 25. cikkében meghatározott követelményeknek, és hogy a tesztkörnyezet minden felhasználását alapos értékelésnek kell alávetni. Ez az 54. cikk (1) bekezdésének b)–j) pontjában szereplő feltételek teljes listájára is vonatkozik.

65. A javaslat 54. cikkében szereplő, az adatok további felhasználásával kapcsolatos néhány további megfontolás arra utal, hogy a tesztkörnyezet működtetése erőforrás-igényes, és ezért reálisan azzal kell számolni, hogy csak kevés vállalkozás kapna lehetőséget a részvételre. A tesztkörnyezetben való részvétel versenyelőnyt jelenthet. Az adatok további felhasználásának lehetővé tételéhez alaposan meg kell fontolni, hogy miként válasszák ki a résztvevőket annak biztosítása érdekében, hogy a hatály alá tartozzanak, és elkerülhető legyen a tisztességtelen bánásmód. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos aggodalmát fejezi ki amiatt, hogy az adatok tesztkörnyezetben történő további felhasználásának lehetővé tétele eltér az általános adatvédelmi rendeletben alkalmazott elszámoltathatósági megközelítéstől, amelynek keretében az elszámoltathatóság az adatkezelőre, nem pedig az illetékes hatóságra hárul.

66. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos úgy véli továbbá, hogy a tesztkörnyezet célkitűzéseire – azaz az MI-rendszerek fejlesztésére, tesztelésére és hitelesítésére – tekintettel a tesztkörnyezetek nem tartozhatnak a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv hatálya alá. Jóllehet a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv rendelkezik az adatok tudományos kutatási célból történő további felhasználásáról, az e másodlagos célból kezelt adatokra már az általános adatvédelmi rendeletet vagy az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendeletet, nem pedig a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet kell alkalmazni.

67. Nem egyértelmű, hogy mit foglal majd magában a szabályozási tesztkörnyezet. Felmerül a kérdés, hogy a javasolt szabályozási tesztkörnyezet tartalmaz-e minden egyes tagállamban egy informatikai infrastruktúrát, további jogalapokkal a további adatkezeléshez, vagy az csupán a szabályozási szakértelemhez és iránymutatáshoz való hozzáférést szervezi meg. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos szorgalmazza, hogy a jogalkotó pontosítsa ezt a fogalmat a javaslatban, és egyértelműen mondja ki, hogy a szabályozási tesztkörnyezet nem jelent kötelezettséget az illetékes hatóságok számára a műszaki infrastruktúra biztosítására. Az ilyen pontosításnak megfelelően minden esetben az illetékes hatóságok rendelkezésére kell bocsátani a pénzügyi és emberi erőforrásokat.

68. Végezetül az Európai Adatvédelmi Testület és az európai adatvédelmi biztos hangsúlyozni szeretné a határokon átnyúló MI-rendszerek fejlesztését, amelyek az európai digitális egységes piac egésze számára elérhetők lesznek. Az ilyen MI-rendszerek esetében a szabályozási tesztkörnyezet mint az innováció eszköze nem válhat a határokon átnyúló fejlesztés akadályává. A Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezért összehangolt, határokon átnyúló megközelítést javasol, amely nemzeti szinten még mindig kellően elérhető valamennyi kkv számára, és Európa-szerte közös keretet kínál anélkül, hogy túlzottan korlátozó jellegű lenne. Egyensúlyt kell teremteni az európai koordináció és a nemzeti

eljárások között annak érdekében, hogy elkerülhető legyen a jövőbeli MI-rendelet ellentmondásos végrehajtása, ami gátolná az uniós szintű innovációt.

3.3 Átláthatóság

69. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli, hogy a nagy kockázatú MI-rendszereket regisztrálni kell (a javaslat 51. és 60. cikkében említett) nyilvános adatbázisban. Ezt az adatbázist lehetőségnek kell tekinteni arra, hogy a széles nyilvánosságot tájékoztassák az MI-rendszer alkalmazási köréről, valamint azokról az ismert hibákról és váratlan eseményekről, amelyek veszélyeztethetik működését, valamint a szolgáltatók által azok kezelése és orvoslása érdekében elfogadott korrekciós intézkedésekről.

70. Az egyik legfontosabb demokratikus elv a fékek és ellensúlyok alkalmazása. Ezért az a körülmény, hogy az átláthatósági kötelezettség nem vonatkozik a bűncselekmények felderítésére, megelőzésére, kivizsgálására vagy eljárás indítására használt MI-rendszerekre, túlságosan széles körű kivételt képez. Különbséget kell tenni a felderítésre vagy megelőzésre használt MI-rendszerek és az olyan MI-rendszerek között, amelyek célja a bűncselekmények kivizsgálása vagy az eljárás indításának elősegítése. A megelőzésre és felderítésre vonatkozó biztosítékoknak az ártatlanság vélelme miatt erősebbeknek kell lenniük. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezenkívül sajnálatát fejezi ki amiatt, hogy a javaslat nem tartalmaz figyelmeztetéseket, ami úgy értelmezhető, hogy zöld utat kap a még nem bevált, nagy kockázatú MI-rendszerek vagy -alkalmazások használata.

71. Azokban az esetekben, amelyekben titoktartási okokból alig vagy egyáltalán nem biztosítható az átláthatóság a nyilvánosság számára, még egy megfelelően működő demokráciában is biztosítékokra van szükség, és ezeket az MI-rendszereket regisztrálni kell az illetékes felügyeleti hatóságnál, és biztosítani kell számára az átláthatóságot.

72. Az MI-rendszerek átláthatóságának biztosítása nagy kihívást jelentő cél. Számos MI-rendszer teljes mértékben kvantitatív döntéshozatali megközelítése, amely eredendően eltér a többnyire ok-okozati és elméleti érvelésen alapuló emberi megközelítéstől, ellentmondásba kerülhet azzal az igénnyel, hogy a gépi eredményekre előzetes, érthető magyarázatot kell kapni. A rendeletnek elő kell mozdítania az MI-rendszerek felhasználóinak a rendszer mindenkori (döntéshozatali) státuszáról való tájékoztatásának új, proaktívabb és időszerű módjait, korai előrejelzést biztosítva az esetleges káros következményekről, hogy azok az egyének, akiknek jogait és szabadságait csorbíthatják az autonóm gépi döntések, reagálhassanak, vagy orvosolhassák a döntést.

3.4 Az adatok különleges kategóriáinak és a bűncselekményekkel kapcsolatos adatok kezelése

73. Az adatok különleges kategóriáinak a bűnüldözés területén történő kezelését az uniós adatvédelmi keret rendelkezései szabályozzák, ideértve a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvet és annak nemzeti végrehajtását is. A javaslat azt állítja, hogy nem teremt általános jogalapot a személyes adatok kezelésére, ideértve a személyes adatok különleges kategóriáit is (lásd a (41) preambulumbekezdést). A javaslat 10. cikkének (5) bekezdése ugyanakkor kimondja, hogy „az ilyen rendszerek szolgáltatói kezelhetik a személyes

adatok különleges kategóriáit”. Ugyanez a rendelkezés emellett további biztosítékokat követel meg, és példákkal is szolgál. Úgy tűnik tehát, hogy a javaslat összeütközésbe kerül az általános adatvédelmi rendelet, a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet alkalmazásával. Bár az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli a megfelelő biztosítékok kialakítására irányuló kísérletet, koherensebb szabályozási megközelítésre van szükség, mivel a jelenlegi rendelkezések nem tűnnek kellően egyértelműnek ahhoz, hogy jogalapot teremtsenek az adatok különleges kategóriáinak kezelésére, és azokat további, még értékelendő védelmi intézkedésekkel kell kiegészíteni. Ezenfelül ha a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv hatálya alá tartozó adatkezelés útján személyes adatok gyűjtésére került sor, figyelembe kell venni a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv nemzeti átültetéséből eredő esetleges további biztosítékokat és korlátozásokat is.

3.5 Megfelelési mechanizmusok

3.5.1 Tanúsítás

74. A javaslat egyik fő pillére a tanúsítás. A javaslatban felvázolt tanúsítási rendszer a szervezetek struktúráján (bejelentő hatóságok/bejelentett szervezetek/Bizottság) és a magas kockázatú MI-rendszerekre vonatkozó kötelező követelményeket lefedő, valamint az 1025/2012/EU rendelet szerinti harmonizált európai szabványokon és a Bizottság által meghatározandó egységes előírásokon alapuló megfelelőségértékelési/tanúsítási mechanizmuson alapul. Ez a mechanizmus eltér az általános adatvédelmi rendelet 42. és 43. cikkében körvonalazott, az adatvédelmi szabályoknak és elveknek való megfelelés biztosítását szolgáló tanúsítási rendszertől. Nem egyértelmű azonban, hogy a bejelentett szervezetek által a javaslatnak megfelelően kiadott tanúsítványok hogyan kapcsolódhatnak az általános adatvédelmi rendelet szerinti adatvédelmi tanúsítványokhoz, bélyegzőkhöz és jelölésekhez, eltérően attól, amit a javaslat más típusú tanúsítványok esetében előír (lásd a 42. cikk (2) bekezdését az (EU) 2019/881 rendelet alapján kiadott tanúsítványok tekintetében).

75. Amennyiben a magas kockázatú MI-rendszerek személyes adatok kezelésén alapulnak, vagy személyes adatokat kezelnek feladatuk ellátása érdekében, ezek az eltérések jogbizonytalanságot eredményezhetnek valamennyi érintett szervezet számára, mivel olyan helyzetekhez vezethetnek, amelyekben a javaslat alapján tanúsított és CE megfelelőségi jelöléssel ellátott MI-rendszereket forgalomba hozatalukat vagy üzembe helyezésüket követően olyan módon lehet használni, amely nem felel meg az adatvédelmi szabályoknak és elveknek.

76. A javaslat nem mutat egyértelmű kapcsolatot az adatvédelmi joggal, valamint a III. mellékletben felsorolt nagy kockázatú MI-rendszerek egyes „területeire” alkalmazandó egyéb uniós és tagállami jogszabályokkal. A javaslatba bele kell foglalni különösen az adattakarékosság és a beépített adatvédelem elvét mint a CE-jelölés megszerzése előtt figyelembe veendő szempontok egyikét, tekintettel arra, hogy a nagy kockázatú MI-rendszerek potenciálisan nagymértékben beavatkoznak a magánélethez és a személyes adatok védelméhez való alapvető jogba, valamint hogy biztosítani kell az MI-rendszerbe vetett magas szintű bizalmat. Ezért az Európai

Adatvédelmi Testület és az európai adatvédelmi biztos javasolja a javaslat módosítását az említett rendelet alapján kiadott tanúsítványok és az adatvédelmi tanúsítványok, bélyegzők és jelölések közötti kapcsolat pontosítása érdekében. Végül az adatvédelmi hatóságokat be kell vonni a harmonizált szabványok és egységes előírások kidolgozásába és elfogadásába.

77. A javaslat megfelelőségértékeléssel kapcsolatos 43. cikkével összefüggésben a 47. cikkben meghatározott megfelelőségértékelési eljárástól való eltérés igen széles körűnek tűnik, és túl sok kivételt foglal magában, mint például a közbiztonság vagy a személyek életének és egészségének védelmét, a környezetvédelmet, valamint a kulcsfontosságú ipari és infrastrukturális eszközök védelmét szolgáló kivételes okokat. Javasoljuk a jogalkotóknak e kivételek szűkítését.

3.5.2 Magatartási kódexek

78. A javaslat 69. cikke szerint a Bizottság és a tagállamok ösztönzik és elősegítik olyan magatartási kódexek kidolgozását, amelyek célja, hogy előmozdítsák a nagy kockázatú MI-rendszerekre vonatkozó követelményeknek, valamint további követelményeknek a nem nagy kockázatú MI-rendszerek szolgáltatói általi önkéntes alkalmazását. Az általános adatvédelmi rendelet (78) preambulumbekezdésével összhangban az Európai Adatvédelmi Testület és az európai adatvédelmi biztos azt ajánlja, hogy azonosítsák és határozzák meg az ezen eszközök és az általános adatvédelmi rendeletben előírt, az adatvédelmi megfelelést támogató magatartási kódexek közötti szinergiákat. Ebben az összefüggésben fontos pontosítani, hogy a személyes adatok védelmét a 69. cikk (2) bekezdésében említett magatartási kódexek által kezelhető „további követelmények" közé kell-e sorolni. Azt is fontos biztosítani, hogy a 69. cikk (1) bekezdésében említett magatartási kódexek által kezelt „műszaki előírások és megoldások", amelyek célja az MI-rendelettervezet követelményeinek való megfelelés előmozdítása, ne ütközzenek az általános adatvédelmi rendelet és az európai uniós intézményekre, hivatalokra, szervekre és ügynökségekre vonatkozó adatvédelmi rendelet szabályaiba és elveibe. Ezáltal ezen eszközöknek a nem nagy kockázatú MI-rendszerek szolgáltatói által történő tiszteletben tartása – amennyiben az említett rendszerek személyes adatok kezelésén alapulnak, vagy feladataik ellátása érdekében személyes adatokat kezelnek – hozzáadott értéket képviselne, mivel biztosítja, hogy az adatkezelők és az adatfeldolgozók képesek lesznek eleget tenni adatvédelmi kötelezettségeiknek e rendszerek használata során.

79. Ugyanakkor a megbízható MI-re vonatkozó jogi keretet kiegészítené a magatartási kódexek integrálása, hogy előmozdítsa az e technológia biztonságos és jogkövető használatába vetett bizalmat, ideértve az alapvető jogok tiszteletben tartását is. Ezen eszközök kialakítását azonban meg kell erősíteni olyan mechanizmusok előírásával, amelyek célja annak ellenőrzése, hogy ezek a kódexek hatékony „műszaki előírásokat és megoldásokat" nyújtanak-e, és a szóban forgó kódexek szerves részeként „egyértelmű célkitűzéseket és az említett célkitűzések elérésének mérésére szolgáló fő teljesítménymutatókat" határoznak meg. Ezenkívül a magatartási kódexek tekintetében az olyan (kötelező) nyomonkövetési mechanizmusokra való hivatkozás hiánya, amelyek célja annak ellenőrzése, hogy a nem nagy kockázatú MI-rendszerek szolgáltatói megfelelnek-e a kódexekben foglalt rendelkezéseknek, valamint az a lehetőség, hogy az egyes szolgáltatók (maguk) dolgozzák ki (és alkalmazzák) az említett kódexeket (lásd az indokolás 5.2.7. szakaszát), tovább gyengítheti ezen eszközök hatékonyságát és végrehajthatóságát.

80. Végezetül az Európai Adatvédelmi Testület és az európai adatvédelmi biztos pontosítást kér azon kezdeményezések típusait illetően, amelyeket a Bizottság a javaslat (81) preambulumbekezdése szerint „azon technikai akadályok csökkentésének megkönnyítése érdekében [dolgozhat ki], amelyek gátolják a mesterséges intelligencia fejlesztésére irányuló, határokon átnyúló adatcserét".

4 KÖVETKEZTETÉS

81. Bár az Európai Adatvédelmi Testület és az európai adatvédelmi biztos üdvözli a Bizottság javaslatát, és úgy véli, hogy egy ilyen rendeletre szükség van az uniós polgárok és lakosok alapvető jogainak biztosításához, véleményük szerint a javaslatot több kérdésben is ki kell igazítani alkalmazhatóságának és hatékonyságának biztosítása érdekében.

82. A javaslat összetettségére és az általa kezelni kívánt kérdésekre tekintettel még sok a tennivaló addig, amíg a javaslat megfelelően működő jogi keretet teremthet, amely hatékonyan kiegészíti az általános adatvédelmi rendeletet az alapvető emberi jogok védelme terén, előmozdítva ugyanakkor az innovációt. Az Európai Adatvédelmi Testület és az európai adatvédelmi biztos a továbbiakban is készen áll arra, hogy támogatást nyújtson ezen az úton.

Brüsszel, 2021. június 18.

Az Európai Adatvédelmi Testület részéről	Az európai adatvédelmi biztos részéről
Az elnök	Az adatvédelmi biztos
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI