Jog-Állam-Politika, 2024/4.277
DOI: 10.58528/JAP.2024.16-4.277

FÓRUM

SZABÓ HEDVIG

„Valós idejű" távoli biometrikus azonosítás és jogi szabályozás: A Mesterséges Intelligencia Rendelet alkalmazása Magyarországon

ABSTRACT

Addressing the legal challenges associated with real-time remote biometric identification systems requires regulatory action in Hungary. The European Union's Artificial Intelligence Regulation, which came into effect on August 1, 2024, mandates compliance for remote biometric identification systems by February 1, 2025. The regulation aims to prohibit the use of real-time remote biometric identification systems in public spaces for law enforcement purposes, with specific exceptions. The EU allows the use of these systems for law enforcement purposes under strict conditions, including the requirement for human oversight in the biometric identification decision-making processes. However, the legal framework protecting fundamental rights needs adjustments within the Hungarian legal system. This study summarises the provisions of the EU regulation and analyses the Hungarian legislative environment, identifying gaps and proposing necessary amendments to align with EU regulations. The potential of real-time remote biometric identification systems in ensuring public safety is also acknowledged.

Keywords: Artificial Intelligence Regulation ■ biometric identification ■ fundamental rights ■ law enforcement

I. BEVEZETÉS

A biometrikus azonosítás a modern biztonságtechnológia egyik leginnovatívabb és leggyorsabban fejlődő területe. A technológia célja az egyének egyedi fiziológiai jellemzői alapján történő azonosítása és hitelesítése. Az elmúlt években a biometrikus rendszerek alkalmazása jelentősen növekedett, a kormányzati szférában és a mindennapi élet különböző területein is.

A biometrikus azonosítás alapelve az, hogy minden egyén rendelkezik olyan egyedi fizikai jellemzőkkel, mint például az ujjlenyomat, az írisz- vagy retinaminta, az arc; vagy olyan viselkedési mintázatokkal,

mint az aláírás vagy a gépelési ritmus, amelyek alkalmasak a személyek egyértelmű azonosítására.[1] Ezen technológiák egyik legnagyobb előnye, hogy nehéz őket hamisítani vagy ellopni, mivel az azonosításhoz használt jellemzők szorosan kapcsolódnak az egyén biológiai vagy viselkedési sajátosságaihoz. Az utóbbi évek technológiai fejlődése, a mesterséges intelligencia alkalmazása a biometrikus rendszerekben tovább növelték az azonosítás pontosságát és megbízhatóságát.

A bűnüldözés mellett sem haladtak el észrevétlenül az új technológiák.[2] A rendvédelmi szervek megkezdték ezek használatát, már csak amiatt is, mert a közvélemény elvárja, hogy az állami szervek eredményesen és egyben költséghatékonyan működjenek, ahol csak lehetséges, gazdasági eredményességet mutassanak és csökkentsék a munkaerő költségeket, amelyet elsősorban az új technológiák bevezetése segíthet elérni.[3] Az elmúlt évtizedben számos új technológiát vettek igénybe a bűnüldöző szervek, többek között a térfigyelő kamerákat, automatikus rendszámfelismerő rendszereket, testkamerákat, drónokat és nem utolsó sorban arcfelismerő technológiákat.

Az arcfelismerő technológia alkalmazása mellett döntöttek a 2024-es párizsi olimpián is. A 2024-1017 számú rendelet értelmében a párizsi közlekedési vállalat 46 állomásán engedélyezték az algoritmikus képfeldolgozás alkalmazását a videomegfigyelési rendszer képein 2024. július 22. és 2024. augusztus 12. között.[4] A döntés hullámokat vetett a jogvédelemmel foglalkozó szervezeteknél.[5]

A fentiek is megerősítik, hogy a technológia széleskörű alkalmazása új kihívásokat hozott, elsősorban az alapvető jogok tekintetében. A biometrikus adatok kezelése és védelme kritikus fontosságú, mivel ezek az adatok rendkívül érzékenyek, és azok nem megfelelő kezelése esetén súlyos következményekkel járhatnak az érintettek számára. Újhegyi Péter 2022-es kutatása, melyben a biometria elterjedését, az elterjedést gátló tényezőket és a felhasználók érzelmi és gondolati attitűdjét vizsgálta, alátámasztotta, hogy az egyének valóban veszélyként tekintenek a biometrikus azonosításra. Megállapította, hogy a „biometrikus rendszerek elfogadottsága az elmúlt nyolc évben szignifikánsan romlott. Kijelenthető, hogy a biometrikus azonosítási módszerek elterjedésének legfőbb gátja a széles körű társadalmi elfogadás hiánya."[6] A biometrikus azonosításhoz kötődő társadalmi percepciót az Európai Unió is észlelte, és ennek megfelelően hozott meglehetősen szigorú rendelkezéseket a mesterségesintelligencia-rendszereken belül, a biometrikus azonosításra szolgáló megoldásokkal kapcsolatban.

Jelen tanulmány célja, hogy átfogó képet nyújtson a „valós idejű" távoli biometrikus azonosítás alkalmazásában rejlő jogi kihívásokról, a magyar szabá-

[1] Bolle – Connell – Pankanti – Ratha – Senior, 2013.
[2] Vájlok – Balla – Bartus – Vedó, 2022.
[3] Ratnaparkhi – Tandasi – Saraswat, 2021.
[4] Recueil Des Actes Administartifs Special N° 75-2024-440 Publié le 19 Juilliet 2024 Prefectura de Paris.
[5] Wired.com: At the Olympics, AI Is Watching You, 2024.
[6] Ujhegyi, 2023, 1463-1491.

lyozás előtt álló kihívásokról. A téma különösen időszerű, mert az Európai Unió Mesterséges Intelligencia Rendelete (továbbiakban: Rendelet) 2024. augusztus 01-én hatályba lépett, és a távoli biometrikus azonosító rendszerek esetében 2025. február 1-tól alkalmazni kell.

II. „VALÓS IDEJŰ" TÁVOLI BIOMETRIKUS AZONOSÍTÁS A RENDELET ALAPJÁN

A Rendelet alapelgondolása, hogy a tiltott mesterségesintelligencia-gyakorlatok közé sorolja a „valós idejű" távoli biometrikus azonosító rendszerek használatát a nyilvánosság számára hozzáférhető helyeken bűnüldözési célokból, kivételek meghatározásával.[7]

1. Biometria

Elsőként érdemes egyértelműsíteni, hogy mit is tekintünk biometriának. Hazainé meghatározásában a biometria klasszikus megközelítése a személyek egyedi biológiai – fiziológiai és viselkedésbeli tulajdonságainak mérésén alapuló elemzést és azonosítást jelenti, matematikai és biostatisztikai módszerekkel. Azonban az IKT-technológia és gépi tanulás fejlődésével a modern definíció már az automatikus folyamatokat hangsúlyozza. A biometrikus azonosítás az ember fizikai, fiziológiai, viselkedési és pszichológiai jellemzőinek gépi úton történő felismerését és ezen adatok összehasonlítását jelenti az adatbázisban tárolt biometrikus adatokkal, az egyén azonosságának megállapítása céljából, különböző technológiák és módszerek alkalmazásával.[8] A Rendelet a „távoli biometrikus azonosító rendszer" fogalmát nem technológiai alapon, hanem funkcionális értelemben határozza meg, olyan MI-rendszerként, amelynek célja természetes személyek azonosítása, anélkül, hogy azok aktívan részt vennének az azonosítási eljárásban, általában távolról, az adott személy biometrikus adatainak egy referencia-adatbázisban tárolt biometrikus adatokkal való összevetésével.[9] Ez a meghatározás független az alkalmazott technológiától, folyamatoktól vagy a biometrikus adatok típusától. Az ilyen távoli biometrikus azonosító rendszereket általában több személy, illetve azok viselkedésének egyidejű észlelésére használják, jelentősen megkönnyítve a természetes személyek azonosítását aktív közreműködésük nélkül.

A Rendelet hatálya azonban nem terjed ki azokra a biometrikus ellenőrzésre szánt MI-rendszerekre, amelyek hitelesítési céllal működnek, és kizárólag azt erősítik meg, hogy egy adott természetes személy valóban az, akinek állítja magát. Ezek

[7] Rendelet 5. cikk.
[8] Hazai, 2024.
[9] Rendelet (15).

a rendszerek arra szolgálnak, hogy megerősítsék a személyazonosságot olyan célokból, mint például egy szolgáltatás igénybevétele, egy eszköz zárolásának feloldása vagy biztonsági hozzáférés biztosítása egy helyiséghez. Ezen rendszerek kizárása a tiltott alkalmazások közül azzal indokolható, hogy az ilyen rendszerek valószínűleg csak csekély hatást gyakorolnak a természetes személyek alapvető jogaira, ellentétben a nagy számú személy biometrikus adatainak – aktív közreműködésük nélkül történő – kezelésére használható távoli biometrikus azonosító rendszerekkel.[10]

2. Valósidejűség

Egy biometrikus azonosítási rendszer akkor válik tiltottá, ha valós idejű. A valós idejű rendszerek esetében a biometrikus adatok rögzítése, az összehasonlítás és az azonosítás azonnal, majdnem azonnal, de semmiképp nem jelentős késleltetés nélkül történik. A valósidejűség kikerülése érdekében nem lehet kisebb késleltetést építeni a rendszerbe. A valós idejű rendszerek élő vagy megközelítőleg élő anyagot, például videofelvételt használnak, amelyet kamera vagy más hasonló funkciójú eszköz generál.

A nem valós idejű vagy utólagos rendszerek esetében a biometrikus adatokat már rögzítették, az összevetésre és az azonosításra csak jelentős késleltetéssel kerül sor. Ezek a rendszerek olyan forrásokból származhatnak, mint a zártláncú televíziós kamerák, de bármilyen technológiával előállított képek vagy videofelvételek lehetnek, amelyek az azonosítással érintett természetes személyek esetében már az azonosítás előtt készültek.

3. Bűnüldözési cél

A „valós idejű" távoli biometrikus azonosító rendszerek nyilvános helyeken történő bűnüldözési célú használata csak az alábbi esetekben megengedett, ha és amennyiben ez az alábbi célok egyikéhez feltétlenül szükséges:

- Konkrét áldozatok célzott felkutatása emberrablás, emberkereskedelem vagy szexuális kizsákmányolás esetén, valamint eltűnt személyek felkutatása.
- Konkrét, jelentős és közvetlen veszély megelőzése, amely természetes személyek életét vagy fizikai biztonságát fenyegeti, illetve egy terrortámadás tényleges és valós vagy előre látható veszélyének elhárítása.
- Bűncselekmény elkövetésével gyanúsított személyek lokalizálása vagy azonosítása nyomozás vagy büntetőeljárás lefolytatása, illetve büntetőjogi szankció végrehajtása céljából olyan bűncselekmények esetében, amelyeket a II. melléklet említ, és amelyekért az érintett tagállamban a

[10] Rendelet (15).

büntetési tétel felső határa legalább négyévi szabadságvesztés vagy szabadságelvonással járó intézkedés.[11]

A bűncselekmények tárgya szerinti küszöbérték biztosítja, hogy a bűncselekmény kellően súlyos legyen ahhoz, hogy indokolhassa a „valós idejű" távoli biometrikus azonosító rendszerek használatát.

Ezek a bűncselekmények a 2002/584/IB tanácsi kerethatározatban felsorolt 32 bűncselekményen alapulnak, figyelembe véve, hogy némelyik relevánsabb lehet a gyakorlatban, azaz a „valós idejű" távoli biometrikus azonosítás szükségessége és arányossága változhat a különböző bűncselekmények esetén.[12] Ezt befolyásolhatja a kár súlyosságának, valószínűségének és mértékének különbsége, valamint a bekövetkezés esetleges negatív hatásainak eltérése.

A természetes személyek életét vagy testi biztonságát fenyegető közvetlen veszély a kritikus infrastruktúrát érintő súlyos zavarokból is fakadhat, ha az ilyen infrastruktúra megzavarása vagy megsemmisítése közvetlen veszélyt jelentene a személyek életére vagy testi biztonságára, például az alapvető ellátások biztosításának vagy az állam alapvető funkciói gyakorlásának súlyos sérelme miatt.[13]

Továbbá a Rendeletnek nem célja, hogy az eddigi, megfelelő jogalapon működő rendszerek használatában korlátozás legyen, ennek alapján biztosítania kell, hogy a bűnüldöző hatóságok képesek legyenek személyazonosság-ellenőrzést végezni az érintett személy jelenlétében, az uniós és nemzeti jogszabályokkal összhangban. Lehetővé kell tenni ezeknek a hatóságoknak, hogy az uniós vagy nemzeti joggal összhangban információs rendszereket használjanak azoknak a személyeknek az azonosítására, akik megtagadják az azonosítást, vagy nem tudják igazolni személyazonosságukat. Ez például olyan, bűncselekményben érintett személy esetén is alkalmazható, aki nem hajlandó felfedni személyazonosságát, vagy aki baleset következtében vagy egészségi állapota miatt képtelen erre.

Ez a rendelkezés nem érinti, hogy a biometrikus adatok kezelését csak az (EU) 2016/679 rendelet (GDPR) 9. cikkével összhangban lehet csak megtenni, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, vala-

[11] A II. Mellékletben nevesített bűncselekmények: terrorizmus, emberkereskedelem, gyermekek szexuális kizsákmányolása és gyermekpornográfia, kábítószerek vagy pszichotróp anyagok tiltott kereskedelme, fegyverek, lőszerek és robbanóanyagok tiltott kereskedelme, szándékos emberölés, súlyos testi sértés, emberi szervek vagy szövetek tiltott kereskedelme, nukleáris és radioaktív anyagok tiltott kereskedelme, emberrablás, személyi szabadságtól való jogellenes megfosztás és túszejtés, a Nemzetközi Büntetőbíróság joghatósága alá tartozó bűncselekmények, repülőgép vagy hajó hatalomba kerítése, szexuális kényszerítés, környezettel kapcsolatos bűncselekmények, szervezett vagy fegyveres rablás, szabotázs, a fent felsoroltak közül egy vagy több bűncselekményben érintett bűnszervezetben való részvétel.

[12] A Tanács kerethatározata (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról.

[13] Az Európai Parlament és a Tanács (EU) 2022/2557 Irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről 2. cikkének 4. pontja.

mint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.[14]

4. Nyilvánosság számára hozzáférhető hely

Az alkalmazás szempontjából úgyszintén jelentősége van a „nyilvánosság számára hozzáférhető helyek" kifejezésnek. Ezek a helyek olyan fizikai helyek, amely meghatározatlan számú ember számára elérhetőek, függetlenül attól, hogy magán- vagy köztulajdonban vannak-e, és milyen tevékenységre használhatóak. Így például üzletek, éttermek, bankok, sportlétesítmények, közlekedési eszközök és állomások, szórakozóhelyek, közutak, parkok és játszóterek. Ezek a helyek akkor is hozzáférhetőnek minősülnek, ha belépésükhöz bizonyos feltételek teljesítése szükséges, mint jegyvásárlás, előzetes regisztráció vagy életkori korlátozás. Azonban egy hely nem tekinthető a nyilvánosság számára hozzáférhetőnek, ha hozzáférése közbiztonsági vagy jogi korlátozások alapján konkrét személyekre van korlátozva, vagy ha egyértelmű, hogy a belépés nem engedélyezett (például belépést tiltó táblák). Nyitott ajtó vagy kapu önmagában nem teszi nyilvánosság számára hozzáférhetővé a helyet. Nem nyilvánosság számára nyitott helyek a vállalati és gyárhelyiségek, börtönök, határellenőrzési területek, valamint olyan irodák és munkahelyek, ahova csak az érintett munkavállalók léphetnek be. Vegyes területek, mint egy repülőtér vagy egy magántulajdonú lakóház folyosója, részben hozzáférhetőek lehetnek. De az online terek nem tartoznak ide, mivel nem fizikai helyek. Összeségében a hozzáférhetőséget mindig az adott helyzet sajátosságai alapján kell meghatározni.

5. Alapjogi teszt elvégzése az alkalmazás előtt

A távoli megfigyelés széleskörűen befolyásolhatja a lakosság magánéletét, állandó megfigyelés érzetét keltheti, közvetetten visszatarthatja az embereket a gyülekezési szabadság és más alapvető jogok gyakorlásától.[15] A természetes személyek távoli biometrikus azonosítására szolgáló MI-rendszerek technikai pontatlansága torz eredményekhez vezethet, diszkriminatív hatásokat eredményezhet, amelyek különösen relevánsak lehetnek az életkor, etnikai és faji hovatartozás, nem vagy fogyatékosságok tekintetében.[16] Ezenkívül az ilyen rendszerek azonnali hatása és a kapcsolódó ellenőrzések vagy korrekciók korlátozott lehetőségei fokozott kockázatot jelenthetnek a bűnüldözési tevékenységek által érintett személyek jogaira és szabadságaira nézve.

[14] 9. cikk: A személyes adatok különleges kategóriáinak kezelése.
[15] Németh, 2022.
[16] G. Karácsony, 2019.

A „valós idejű" távoli biometrikus azonosító rendszerek nyilvánosság számára hozzáférhető helyeken történő, bűnüldözési célú használata kizárólag a már említett bűnüldözési célok eléréséhez, a konkrét célszemélyek személyazonosságának megerősítése érdekében indítható el, figyelembe véve a következőket:

- A rendszer használatát indokoló helyzet jellege, különösen az okozott kár súlyossága, valószínűsége és mértéke, ha a rendszer nem kerülne használatra.
- A rendszer használatának az érintett személyek jogaira és szabadságaira gyakorolt következményei, különösen ezen következmények súlyossága, valószínűsége és mértéke.

Annak érdekében, hogy az MI-rendszerek használata felelős és arányos módon történjen, fontos megállapítani, hogy a kimerítően felsorolt és szűken meghatározott helyzetek mindegyikében figyelembe kell venni az alapjogi teszthez szükséges tényezőket. Ezek közé tartozik a kérelem alapjául szolgáló helyzet jellege, az alkalmazás valamennyi érintett személy jogaira és szabadságaira gyakorolt következményei, valamint a használathoz előírt biztosítékok és feltételek.

Az alapjogi teszt Magyarországon az Alaptörvény Szabadság és Felelősség I. cikkének (3) bekezdésén alapul, „az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható."

Az alapjog lényeges tartalma korlátozásának tilalma nem újdonság a magyar jogban, mert már a korábbi Alkotmány is tartalmazta, német modellt követve, 1990 óta hatályos jogként. Az alkotmányos szabályt az Alkotmánybíróság (AB) döntéshozatala során töltötte ki további tartalommal.[17] AB határozatokon keresztül kristályosodott ki, hogy milyen kritériumrendszernek kell, hogy megfeleljen az alapjogi korlátozás, mert önmagában az nem vezethet korlátozáshoz, hogy alkotmányos cél, másik alapjog vagy szabadság védelme indokolja, hanem ezen túl meg kell, hogy feleljen egy úgynevezett arányossági tesztnek is.

A „valós idejű" távoli azonosítást lehetővé tevő rendszerek használata előzetes engedélyhez kötött, amelyet az adott tagállam igazságügyi hatósága vagy független közigazgatási hatósága ad ki. Sürgős esetben az engedély később is megkérhető, legkésőbb 24 órán belül. Az engedély elutasítása esetén a használatot azonnal le kell állítani, és az összes adatot törölni kell. Az engedély csak akkor adható meg, ha az objektív bizonyítékok alapján a rendszer használata szükséges és arányos a cél eléréséhez, és az időtartamra, földrajzi és személyi hatályra korlátozódik. Minden rendszerhasználatról értesíteni kell a Rendelet szerint kijelölt illetékes piacfelügyeleti és az adatvédelmi hatóságokat.

[17] Gáva – Smuk – Téglási, 2017.

A tagállamok dönthetnek úgy, hogy részben vagy teljesen engedélyezik ezen rendszerek használatát, és a szükséges részletes szabályokat nemzeti jogukban rögzítik. A tagállamok értesítik a Bizottságot ezekről a szabályokról, és az uniós jognál szigorúbb jogszabályokat is bevezethetnek. Tagállam alkalmazásra vonatozó pozitív döntése esetén az ilyen rendszerek használata egy tagállam területén csak akkor legyen lehetséges, ha az adott tagállam nemzeti jogszabályaiban kifejezetten rendelkezik az ilyen használat engedélyezésének lehetőségéről. Ennek megfelelően tagállamok arról is dönthetnek, hogy egyáltalán nem engedélyezik az ilyen rendszerek használatát, vagy csak bizonyos, a rendelet által meghatározott célkitűzések tekintetében engedélyezik azt. A szabályozás ugyanakkor nem járhat avval a hatással, hogy kijátszásra kerülnek más, tiltott MI-alkalmazások.

Fontos tisztázni a Rendelet és a bűnügyi adatvédelmi irányelv egymáshoz való viszonyát. Az MI biometrikus azonosítására történő használata bűnüldözési célból szükségszerűen magában foglalja a biometrikus adatok feldolgozását. A Rendelet biometriára vonatkozó szabályait lex specialis-ként kell alkalmazni, a bűnügyi adatvédelmi irányelvben foglalt biometrikus adatkezelési szabályokkal szemben.[18]

Ennek megfelelően, a biometrikus azonosító rendszerek használata és az adatok kezelése csak akkor megengedett, ha az összeegyeztethető a Rendeletben meghatározott kerettel. Az illetékes hatóságok nem használhatják az ilyen rendszereket és nem kezelhetik a kapcsolódó adatokat a bűnügyi adatvédelmi irányelv 10. cikkében felsorolt okokból, ha az kívül esik a Rendelet keretein. Ebben az összefüggésben a Rendeletnek nem célja jogalapot biztosítani a személyes adatok bűnügyi adatvédelmi irányelv 8. cikke[19] szerinti kezeléséhez.

[18] (EU) 2016/680 irányelv 10. cikk: „A személyes adatok különleges kategóriáinak kezelése: A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése csak akkor megengedett, az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciák mellett, ha arra feltétlenül szükség van és:

a) az uniós vagy tagállami jog lehetővé teszi;

b) az érintett vagy más természetes személy létfontosságú érdekeinek védelmét szolgálja; vagy

c) az ilyen adatkezelés olyan adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott."

[19] Az adatkezelés jogszerűsége

(1) A tagállamok biztosítják, hogy az adatkezelés csak akkor és kizárólag annyiban legyen jogszerű, ha és amennyiben olyan feladat ellátásához szükséges, amelyet valamely illetékes hatóság az 1. cikk (1) bekezdésében meghatározott célokból végez, és uniós vagy tagállami jog alapján történik.

(2) Az ezen irányelv hatálya alá tartozó adatkezelést szabályozó tagállami jogban rendelkezni kell legalább az adatkezelés célkitűzéseiről, a kezelendő személyes adatokról és az adatkezelés céljairól.

6. „Valós idejű" biometrikus azonosítás nem bűnüldözési célból

A biometrikus azonosító rendszerek bűnüldözési céloktól eltérő célokra történő használatára nem vonatkozik a Rendelet bűnüldözési célú használatra vonatkozó szabályozása. Az ilyen, nem bűnüldözési célú használat ezért nem köteles a Rendelet szerinti engedélyezési követelményeknek megfelelni, és nem vonatkoznak rá a nemzeti jogban érvényesülő, ilyen engedélyeket szabályozó részletes előírások. A bűnüldözéstől eltérő célok esetében a GDPR és LED szabályok – a meghatározott kivételek mellett – tiltják a biometrikus adatok kezelését. A nemzeti adatvédelmi hatóságok már hoztak határozatokat a távoli biometrikus azonosítás bűnüldözéstől eltérő célokra történő használatának tiltására.[20]

Bár nem uniós ország már, de adatvédelmi gyakorlatában az uniós elveket követi az Egyesült Királyság Adatvédelmi Hatósága – a GDPR és az bűnügyi adatvédelem érvényesítéséért felelős kormányzati szerv –, amely független vizsgálatot indított a londoni King's Cross pályaudvaron használt arcfelismerés miatt, miután kiderült, hogy a nyilvánosság beleegyezése nélkül szkennelték az emberek arcát. Ez a botrány országszerte leállította a rendőrségi biometrikus rendszerek alkalmazását, míg a South Wales-i rendőrséget hasonló ügy miatt bíróság elé is állították.[21]

A távoli biometrikus azonosító rendszerek alkalmazásával kapcsolatos kockázatok súlyosságát a Clearview AI esete jól példázza. A francia adatvédelmi hatóság, a CNIL 2020 májusától több panaszt kapott a Clearview AI arcfelismerő szoftverével kapcsolatban. Ezek a panaszok arra vonatkoztak, hogy a cég gyakorlata sérti az érintettek adatvédelmi jogait, és nem tesz eleget a GDPR követelményeinek.

A CNIL vizsgálatot indított, és 2021 novemberében hivatalos felszólítást küldött a Clearview AI-nak, hogy szüntesse meg a francia területen tartózkodó érintettek személyes adatainak jogalap nélküli gyűjtését és kezelését, és biztosítsa az érintettek jogainak gyakorlását, beleértve a személyes adatok törlésére vonatkozó kérelmek teljesítését. A Clearview AI azonban nem válaszolt a felszólításra. Ennek következtében a CNIL 20 millió eurós pénzbírságot szabott ki a Clearview AI ellen. Emellett a hatóság kötelezte a céget, hogy szüntesse meg a jogalap nélküli adatgyűjtést és adatkezelést, és törölje az érintett személyes adatokat. A hatóság továbbá napi 100 000 eurós bírságot helyezett kilátásba a kötelezettségek teljesítésének elmulasztása esetére.[22]

Továbbá, magyar esetben a NAIH is indított eljárást Siófokon, ahol közterületi kamerarendszer arcfelismerő technológia használatának gyanúja merült fel. Bár az arcfelismerés nem bizonyosodott be, több jogsértést is megállapítottak, így bírságot szabtak ki és nyilvánosságra hozták az érintett szereplők nevét.[23]

[20] Necz, 2022.

[21] Tooley, 2020.

[22] Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI.

[23] NAIH-963-10/2022.

III. TÁVOLI BIOMETRIKUS AZONOSÍTÁS JOGI LEHETŐSÉGE MAGYARORSZÁGON

A Rendelet alapján számos jogalkotási feladat vár valamennyi tagállamra, de a legsürgetőbb a távoli biometrikus azonosítás kérdésének jogi rendezése, melynek 2025. február 1-vel meg kell történnie.

Ha a magyar jogi környezetet vizsgáljuk, a következő rendvédelemre vonatkozó hatályos jogszabályokat találjuk, amelyek összefüggésbe hozhatóak a távoli biometrikus azonosítás kérdésével. A rendőrség számára az Rtv. 42. § (2) bekezdése biztosítja „képfelvevő – bárki számára nyilvánvalóan észlelhető módon történő – elhelyezését és felvétel készítését, az olyan közterületen, ahol az közbiztonsági, bűnmegelőzési, illetve bűnüldözési célból igazolhatóan szükséges".[24] Ez a rendelkezés nem a távoli biometrikus azonosítást szabályozza, csak képfelvétel-készítést, amellyel kapcsolatban a már idézett siófoki ügyben a NAIH megállapította, hogy „az Rtv. 42. § (2) rendelkezése, amely lehetőséget biztosít a rendőrség számára közterületen képfelvétel készítésére, jogalapot teremt a személyes adatok kezeléséhez. Azonban a közterületen elhelyezett képfelvevők és a képfelvételek készítésének lehetőségére vonatkozó ezen rendelkezések nem értelmezhetők úgy, hogy azok egyben felhatalmazást adnak a szigorúbb adatkezelési feltételek és garanciák alá tartozó biometrikus adatok, mint különleges adatok kezelésére. A jogalkotó célja ezen törvényi rendelkezések megalkotásakor nem az volt, hogy lehetővé tegye az arcfelismerés alkalmazásával történő biometrikus adatok kezelését."

A Be. 207. §. (5) a szemle szabályai között rendezi, hogy „ha a büntetőeljárás során az elkövető azonosítása érdekében biometrikus minta rögzítése indokolt, az ügyészség vagy a nyomozó hatóság az érintett személlyel, tárggyal, helyszínnel vagy tárgyi bizonyítási eszközzel kapcsolatba került személyektől biometrikus mintát rögzíthet más biometrikus minta vétlen szennyeződésének kiszűrése érdekében." A szemle szabályai nem a távoli biometrikus azonosítás kérdését rendezik.[25]

A Be. 269. §. szerint „az ügyészség, a nyomozó hatóság, illetve a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve a törvényben meghatározottak szerint a bűnügyi és rendészeti biometrikus adatok nyilvántartásából adattovábbítást kérhet, valamint az arcképelemzési nyilvántartás vezetéséért és az arcképelemző rendszer működtetéséért felelős szerv arcképelemző tevékenységét veheti igénybe".

Az arcképelemző tevékenység során az arcképelemző tevékenységet végző szerv csak akkor folytathat arcképelemzést a jogosult szerv kérelmére, ha az igénybevételre jogosult szerv pontosan megjelöli az arcképelemzési tevékenység célját, megadja az ügy azonosítását szolgáló adatokat, és az igénybevételt egy írásban felhatalmazott személy kezdeményezi. Az arcképelemző szerv automatizált eljárásban, rendszer–rendszer kapcsolat útján továbbított arcképmások-

[24] A rendőrségről szóló 1994. évi XXXIV. törvény.

[25] A büntetőeljárásról szóló 2017. évi XC. törvény.

ból arckép-profilt készít a rendőrségi feladatok ellátása érdekében. Az arcképelemző tevékenységet végző szerv ezeket az arckép-profilokat összehasonlítja az igénybevételre jogosult szerv által továbbított technikaikapcsoló-számhoz tartozó arckép-profillal, az arcképelemző rendszer segítségével.[26] Az arckép-elemző tevékenység úgyszintén nem a távoli biometrikus azonosítást szabályozza a rendvédelmi szervek vonatkozásában.

Az Infotv. a biometrikus adatokat a személyes adat különleges adat kategóriájaként kezeli. A bűnüldözési célú adatkezelés a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – (bűnüldözési cél) végzett adatkezelése.[27] Különleges adat akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli. Az Infotv. szerint a bűnügyi személyes adatok kezelése esetén – ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik – a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni.

Ezen jogszabályok alapján levonhatjuk azt a következtetést, hogy a távoli biometrikus azonosításnak jelenleg nincsenek meg azok a részletszabályai, amelyek a Rendelet alapján kötelezőek lesznek. Ennek megfelelően a magyar jogalkotásnak el kell készíteni a „valós idejű" távoli biometrikus azonosításra vonatkozó részletszabályokat.

1. Jogalkotói döntési lehetőségek a Rendelet alapján a „valós idejű" biometrikus azonosításról

A Rendelet alapján a tagállamok dönthetnek úgy, hogy nem alkalmaznak „valós idejű" távoli biometrikus azonosító rendszereket. Ezt a döntést minden tagállamnak meg kell hozni, ha úgy dönt, hogy nem alkalmazza ezeket a rend-

[26] Az arcképelemzési nyilvántartásról és az arcképelemző rendszerről szóló 2015. évi CLXXXVIII. törvény.

[27] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.).

szereket, akkor az alapvető jogok ezen a téren nem csorbulnak, de a bűnüldözés eszköztárából kiveszünk egy hatékony lehetőséget. Ezt a megoldást azoknak a tagállamoknak érdemes választani, akik nagyon magas szintű közbiztonsággal rendelkeznek. Ha a tagállamok úgy döntenek, hogy a bűnüldözési érdekek érvényesítése érdekében szükség van a „valós idejű" biometrikus azonosításra, akkor azt jogszabályban kell meghatározni, hogy a Rendelet céljai és bűncselekményei közül melyek esetében lehet alkalmazni a „valós idejű" azonosítást.[28]

Hazai jogszabályban egyértelműen fel kell sorolni az összes célt és bűncselekményt, melyek (a Rendelet felhatalmazása alapján) esetén lehet alkalmazni „valós idejű" azonosítást. Az a tagállamok döntése, hogy az engedélyezést teljeskörűen, minden cél és bűncselekmény vonatkozásában, vagy csak részlegesen lehet engedélyezni.

IV. TÁVOLI, „VALÓS IDEJŰ" BIOMETRIKUS AZONOSÍTÁS KÖTELEZŐEN SZABÁLYOZANDÓ ELEMEI

Ha az érintett tagállamok azt a döntést hozzák meg, hogy részlegesen vagy teljeskörűen lehet alkalmazni a „valós idejű" biometrikus azonosítást, akkor a nemzeti jogban meg kell határozni az engedélyek kérelmezésére, kiadására és felhasználására, valamint az azokkal kapcsolatos felügyeletre és jelentéstételre vonatkozó részletes szabályokat. Engedélyek kérelmezése vonatkozásában a Rendelet elvárása, hogy azt az állam igazságügyi hatósága vagy független közigazgatási hatósága – amelynek határozata kötelező erejű – adja ki. Annak érdekében, hogy a Rendelet szabályainak megfelelően lehessen szabályozni a kérdést, érdemes megvizsgálni, hogy ki tekinthető a magyar jogrendben igazságügyi hatóságnak vagy független közigazgatási hatóságnak. Az nem szorul vizsgálatra, hogy a bíróságok ilyennek tekinthetők, de kérdés, hogy rajtuk kívül még ki tekinthető igazságügyi hatóságnak.

[28] Célok: Áldozatok felkutatása: emberrablás, emberkereskedelem vagy szexuális kizsákmányolás áldozatainak célzott felkutatása, valamint eltűnt személyek felkutatása.
Életet vagy biztonságot fenyegető veszélyek megelőzése: Természetes személyek életét vagy fizikai biztonságát fenyegető konkrét, jelentős és közvetlen veszély, illetve terrortámadás tényleges vagy előre látható veszélyének megelőzése.
Bűncselekmények gyanúsítottjainak lokalizálása vagy azonosítása: Bűncselekmények gyanúsítottjainak lokalizálása vagy azonosítása nyomozás vagy büntetőeljárás lefolytatása céljából olyan bűncselekmények esetén, amelyek büntetési tétele az érintett tagállamban legalább négyévi szabadságvesztéssel vagy szabadságelvonással járó intézkedéssel büntetendők, amely bűncselekmények a következőek lehetnek: terrorizmus, emberkereskedelem, gyermekek szexuális kizsákmányolása és gyermekpornográfia, kábítószerek vagy pszichotróp anyagok tiltott kereskedelme, fegyverek, lőszerek és robbanóanyagok tiltott kereskedelme, szándékos emberölés, súlyos testi sértés, emberi szervek vagy szövetek tiltott kereskedelme, nukleáris és radioaktív anyagok tiltott kereskedelme, emberrablás, személyi szabadságtól való jogellenes megfosztás és túszejtés, a Nemzetközi Büntetőbíróság joghatósága alá tartozó bűncselekmények, repülőgép vagy hajó hatalomba kerítése, szexuális kényszerítés, környezettel kapcsolatos bűncselekmények, szervezett vagy fegyveres rablás, szabotázs, a fent felsoroltak közül egy vagy több bűncselekményben érintett bűnszervezetben való részvétel.

Az Európa Unió Bírósága (EUB) egyértelműsítette, hogy az „igazságügyi hatóság" kifejezés nem korlátozódik kizárólag a tagállami bírákra vagy bíróságokra.[29] Ehelyett tágabban kell értelmezni, és vonatkozik azokra a hatóságokra is, amelyek részt vesznek az adott állam igazságszolgáltatásában. De a minisztériumok vagy a rendőrség nem tekinthető ilyen szervnek, mivel ezek a szervek a végrehajtó hatalom részei.

Abban a kérdésben, hogy vajon igazságügyi hatóság lehet-e az ügyészség is, már több tagállam indított eljárást az EUB előtt, az eljárások az európai elfogatóparancs kiadása körüli kérdések tisztázása érdekében indultak. Az EUB pontosan meghatározta, hogy az érintett tagállamok ügyészsége esetében milyen feltételek teljesítése szükséges ahhoz, hogy az európai elfogatóparancs kibocsátása során biztosított legyen az ügyészség függetlensége és a hatékony bírói jogvédelem elveinek tiszteletben tartása.[30] Mivel a tagállami szabályozásokban jelentős eltérések mutatkoznak, valószínű, hogy a közeljövőben az EUB-ot más tagállamok ügyészségei helyzetének vizsgálatára is fel fogják kérni.

A Rendelet és az uniós joggyakorlat alapján a „valós idejű" biometrikus azonosítás engedélyezésére a bírósági engedélyezés minden esetben megfelelő válasz, de az ügyészi engedélyezés is alkalmas lehet. Azonban amennyiben a jogalkotás az ügyészi engedélyezés irányába megy, nagyobb bizonytalansági tényezőt eredményez, mint a bírósági engedélyezés.

Ha a magyar jogrend oldaláról vizsgáljuk, a biometrikus azonosítás engedélyezése szabályozásának lehetőségeit a büntetőeljárás, valamint a rendőrségről szóló törvény keretei közzé célszerű illeszteni.

Az engedélyek kérelmére, kiadására vonatkozó részletszabályok a Be. XXXVIII. fejezetéhez tartoznak, a bírói engedélyhez kötött leplezett eszközök közé. A jelenlegi szabályozás nem a Rendeletnek megfelelő, így javasolt a Rendelet alapján módosítani az alábbi kérdésekben, a szükséges mértékig:

- Az utólagos engedélyezés esetén: a kellően indokolt, sürgős esetek engedélyezésében kell az egyéb eszközök alkalmazásától eltérően rövidebb (24 órás) határidőt megállapítani.
- Az alkalmazás tartama: a Rendelet az időtartam, a földrajzi és személyi hatály tekintetében a feltétlenül szükséges mértéket határozza meg. A Be. szerint legfeljebb 90 napra lehet engedélyezni a leplezett eszközöket, megfontolandó ugyanakkor, hogy a „valós idejű" távoli biometrikus adatkezelés esetén érdemes ennél szűkebb időtartamban meghatározni az engedély maximális időtartamát.
- Az emberi döntés kötelezőségének előírása: A „valós idejű" távoli biometrikus azonosítás alapfunkciója, hogy döntési eredményt produkál. (Az az eredmény, hogy a felismert személy megegyezik a referenciaadatbázisban lévő személlyel.) Az alapvető jogok védelme érdekében szükséges, hogy kizárólag az MI döntése nem járhat jogkövetkezménnyel,

[29] C-625/19. PPU. sz. ügy Openbaar Ministerie kontra XD.

[30] Lehóczki, 2020.

különösen egy személyre nézve hátrányossal nem. Emiatt olyan rendelkezést kell illeszteni a Be-be, mely szerint a „valós idejű" távoli azonosítás esetén emberi felülvizsgálat szükséges, és ez alapján lehet megtenni a szükséges intézkedéseket az érintett személlyel szemben.

A Be-ben való szabályozáson túl ki kell alakítani azt a mechanizmust, mely a hazai piacfelügyeleti és nemzeti adatvédelmi hatóságok részére történő információátadást rendezi. Ennek megfelelő keretet adhatna az Infotv., amelynek keretében szabályozhatóak lennének az értesítés és adatátadás szabályai. Az értesítésnek tartalmaznia kell az EU Bizottság által meghatározott információkat, de nem tartalmazhat érzékeny operatív adatokat.[31] A Bizottság a piacfelügyeleti és adatvédelmi hatóságoktól kapott jelentések alapján összesített jelentésben teszi közé a tagállamok rendszer használatát.

Az Unió a „valós idejű" távoli biometrikus azonosításra vonatkozó szabályok esetén a tagállamoknak lehetővé teszi, hogy a Rendeletnél szigorúbb szabályokat alkossanak. Az előbbiekben javasolt szabályozás megfelel a Rendeletnek, de annál nem alkalmazna szigorúbb elvárásokat, mert az a bűnüldözés lehetőségeit ellehetetleníti.

Miután a jogalkotó elfogadta a szükséges hazai jogszabályokat, ezekről szabályokról legkésőbb azok elfogadása után, 30 nappal értesítenie kell a Bizottságot.

V. JOGALKALMAZÓI KÖTELEZETTSÉGEK A „VALÓS IDEJŰ" TÁVOLI BIOMETRIKUS AZONOSÍTÁSNÁL

A bűnüldöző hatóságnak mint jogalkalmazónak a Rendelet végrehajtása érdekében egyértelműsítenie kell, hogy van-e lehetősége egy MI-rendszeren belül kezelni a valós idejű és a nem valós idejű biometrikus azonosítást. Hiszen eltérő követelményeknek kell megfelelni a valós és nem valós idejű rendszerek esetében. A valós idejű távoli alkalmazások a bűnüldözésben alapvetően tiltott alkalmazások, az előbbiekben ismertetett kivételekkel. A nem „valós idejű" távoli biometrikus azonosítás a Rendelet III. melléklet 6. cikk (2) bekezdésében a nagy kockázatú MI-rendszerek közé tartozik, amennyiben ezek használatát a vonatkozó uniós vagy nemzeti jog engedélyezi.

Megítélésem szerint van jogi lehetőség a nem valós idejű és a valós idejű biometrikus azonosításra ugyanazon MI-rendszer keretében, azaz technológiai szempontból nem kettő rendszer működik párhuzamosan, hanem egy. Alapesetben a nem valós idejű biometrikus azonosítás alkalmazása történik a rendszer keretében, megfeleltetve valamennyi nagy kockázatú rendszerre vonatkozó kö-

[31] A bizottság sablont bocsát a tagállamok és a nemzeti piacfelügyeleti és adatvédelmi hatóságok rendelkezésére, amely tartalmazza az engedély iránti megkeresésekre hozott határozatok és azok eredményeinek információit, amelyeket az illetékes igazságügyi hatóságok hoztak.

vetelménynek. Ha ezeknek a követelményeknek megfelel, és szükségessé válik a valós idejű azonosítás, akkor a jogszerűség biztosítása mellett – megfelelve a Rendeletnek és a jövőbeli hazai szabályozásnak – kerülhet alkalmazásra a valós idejű azonosítás funkció.

Mielőtt a valós idejű biometrikus azonosító rendszert üzemeltetését (nem alkalmazását) megkezdi a bűnüldöző hatóság, el kell végezni az alapjogi hatásvizsgálatot, még a rendszer üzembe helyezése előtt.[32] Az alapjogi hatásvizsgálatnak ki kell terjednie a következő kérdésekre:

- A folyamatok leírása, amelyekben a nagy kockázatú MI-rendszert rendeltetésszerűen használják. A bűnüldöző hatóság folyamatainak leírása relatíve egyszerű, mert erre a kérdésre maga a Rendelet adja meg a választ, hogy egyáltalán milyen esetekben merülhet fel a távoli biometrikus azonosítás lehetősége.
- Az időszak és gyakoriság leírása, amelyen belül a nagy kockázatú MI-rendszereket használni szándékoznak. A nem valós idejű rendszer leírására van lehetőség, mert a valós idejű rendszer használatát előzetes engedély birtokában lehet megkezdeni vagy ezeken kívül, sürgős, kivételes esetben. Ezekben az esetekben az engedélyben kerülnek rögzítésre az időszakkal és a gyakorisággal kapcsolatos információk, így a hatásvizsgálatban azt lehet rögzíteni, hogy az engedélynek megfelelően történjen.
- A rendszer használatával érintett természetes személyek és csoportok kategóriái. A távoli biometrikus azonosító rendszer feltétele, hogy nyilvánosság számára nyitva álló helyen történjen az azonosítás. Ez alapján vélhetően az lesz a beazonosítható kategória, hogy fizikailag hol kerül elhelyezésre az arcfelismerésre alkalmas kamera, pontosan be kell határolni, hogy földrajzilag hol történik a biometrikus azonosítás, pontosan megjelölve, hogy milyen területet lát a kamera, azon a területen milyen emberek és csoportok előfordulása valószínű. (A bevezetőben említett francia olimpiai példában a metróállomások elnevezése kerül megjelölésre, mint földrajzi hely, további részletezettség nélkül.)
- Az érintett személyekre gyakorolt konkrét kárkockázatok lehetősége. A valós idejű biometrikus azonosítás kárkockázata az, hogy a rendszer fals pozitív találatként beazonosít valakit, aki nem azonos a célszeméllyel. Mivel emberi felügyelet alkalmazása kötelező, lehetőség van a rendszer tévedésének korrigálására az ember által. Ha az ember nem tudja korrigálni a rendszer tévedését, mert az ember is téved, akkor az érintett tudja gyakorolni a jogorvoslati lehetőségeit.
- Az emberi felügyeleti intézkedések végrehajtásának leírása a használati utasítás szerint. Mivel kógens rendelkezés, hogy kizárólag a valós idejű távoli biometrikus azonosító rendszer kimenete alapján nem hozható

[32] Rendelet, 27. cikk.

olyan döntés, amely egy személyre nézve hátrányos joghatással jár. Így már a jogalkotónak szabályozni kell, hogy a rendszer alapján jelzett azonosító találat hogyan kerül az ember által felülvizsgálatra.
– A kockázatok bekövetkezése esetén meghozandó intézkedések, beleértve a belső irányítási és panasztételi mechanizmusokat. Hazai jogszabály alapján a kidolgozott jogorvoslati eljárást kell alkalmazni, így az alapjogi hatásvizsgálat jogszabályon alapul.

További elvárás a jogalkalmazóktól, hogy a távoli biometrikus azonosító rendszert még az üzembe helyezés előtt – az alapjogi hatásvizsgálat elvégzése mellett – az Uniós adatbázisba is regisztrálják. A regisztrációs kötelezettség teljesítése nélkül is használatba vehetők ezek a rendszerek, indokolt, sürgős esetekben, amennyiben a regisztráció indokolatlan késedelem nélkül megtörténik.

VI. ZÁRÓ GONDOLATOK

A „valós idejű" távoli biometrikus azonosítás jelentős lehetőségeket és egyben kihívásokat is rejt magában. Az ilyen rendszerek alkalmazása elősegítheti a bűnüldözés hatékonyságát, de komoly alapjogi kérdéseket is felvet. A Rendelet egyértelmű szabályozást ad arra vonatkozóan, hogy milyen keretek között lehet ezeket a rendszereket alkalmazni, figyelemmel a természetes személyek alapvető jogainak védelmére.

Magyarország számára elengedhetetlen, hogy a Rendelet előírásainak megfelelően szabályozza ezt a területet, biztosítva ezzel a biometrikus azonosítás jogszerű és átlátható alkalmazását. A jogalkotói és jogalkalmazói feladatok egyértelműek, a polgárok bizalmának elnyerése és fenntartása érdekében a jogalkotásnak és a technológiai fejlesztéseknek együtt kell haladniuk, biztosítva a legmagasabb szintű alapjogvédelmi garanciákat.

Összességében a távoli biometrikus azonosítás technológiája képes lehet nagyban hozzájárulni a közbiztonság növeléséhez, azonban ennek jogszerű, átlátható és felelősségteljes alkalmazása elengedhetetlen feltétele annak, hogy a társadalom széles körben elfogadja és támogassa ezen technológiák használatát. Az elkövetkező időszak feladata, hogy Magyarország megfeleljen ezeknek a kihívásoknak és lehetőségeknek, biztosítva a jogszabályi környezet folyamatos fejlesztését az új technológiai innovációkhoz.

IRODALOM

• Bolle, Ruud M. – Connell, Jonathan H. – Pankanti, Sharath – Ratha, Nalini K. – Senior, Andrew W. (2013): *Guide to biometrics.* Springer Science & Business Media.

• Gáva Krisztián – Smuk Péter – Téglási András (2017): *Az Alaptörvény értékei – Tudástár.* Dialóg Campus Kiadó, Budapest.
• G. Karácsony Gergely (2019): *A mesterséges intelligenciák szabályozásának közjogi kérdései. A gazdasági jogalkotás aktuális kérdései*. Dialóg Campus Kiadó, Budapest.
• Hazai Lászlóné (2024): A klasszikus biometriától, biostatisztikától az automatikus biometrikus személyazonosság-ellenőrzésig: Út a mesterséges intelligenciáig. In: *Nemzetbiztonsági Szemle.* 12(1).
DOI: https://doi.org/10.32561/nsz.2024.1.5.
• Lehóczki Balázs (2020): Az uniós tagállamok ügyészségei által kibocsátott európai elfogatóparancsok végrehajthatósága. In: *Acta Humana*. 2020/1. sz.
DOI: https://doi.org/10.32566/ah.2020.1.8.
• Necz Dániel (2022): A mesterséges intelligencia felhasználásával történő adatkezelések egyes sajátos szempontjai. In: *Acta Humana – Emberi Jogi Közlemények*. 10(3).
DOI: https://doi.org/10.32566/ah.2022.3.4.
• Németh Ágota (2022): Az arcfelismerés szerepe a bűnügyi munkában. In: *Magyar Rendészet*. 22 (2).
DOI: https://doi.org/10.32577/mr.2022.2.11.
• Ratnaparkhi, Sanika Tanmay – Tandasi, Aamani – Saraswat, Shipra (2021): Face detection and recognition for criminal identification system. In: *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*.
DOI: https://doi.org/10.1109/confluence51648.2021.9377205.
• Tooley, Jason (2020): The future of biometrics in policing worldwide. In: *Biometric Technology Today.* Vol. 1/2020.
DOI: https://doi.org/10.1016/s0969-4765(20)30009-6.
• Ujhegyi Péter (2023): A biometria elterjedésének elemzése. In: *Belügyi Szemle.* 71(8).
DOI: https://doi.org/10.38146/bsz.2023.8.7.
• Vájlok László – Balla József – Bartus Gábor – Vedó Attila (2022): A Biztonsági Technológiák Nemzeti Laboratórium Biztonságos Ország Biztonságos Határ alprojekt. In: *Magyar Rendészet.* 22 (4).
DOI: https://doi.org/10.32577/mr.2022.4.6.
• Wired.com: At the Olympics, AI Is Watching You. 2024. (Elérhető: https://www.wired.com/story/at-the-olympics-ai-algorithms-are-watching-you/. Letöltés ideje: 2024. 08. 01.).

JOGFORRÁSOK

• Magyarország Alaptörvénye (2011. április 25.).
• A büntetőeljárásról szóló 2017. évi XC. törvény.
• Az arcképelemzési nyilvántartásról és az arcképelemző rendszerről szóló 2015. évi CLXXXVIII. törvény.
• Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.).
• A Rendőrségről szóló 1994. évi XXXIV. törvény.
• Az Európai Parlament és a Tanács (EU) 2024/1689 Rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet).

• Az Európai Parlament és a Tanács (EU) 2022/2557 Irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.
• Az Európai Parlament és a Tanács (EU) (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).
• 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.
• A Tanács kerethatározata (2002. június 13.) az európai elfogatóparancsról és a tagállamok közötti átadási eljárásokról.
• Recueil Des Actes Administartifs Special N° 75-2024-440 Publié le 19 Juilliet 2024 Prefectura de Paris (Elérhető: https://www.prefectures-regions.gouv.fr/ile-de-france/ile-de-france/ile-de-france/irecontenu/telechargement/118657/882926/file/recueil-75-2024-440-recueil-des-actes-administratifs-special%20du%2019.07.2024.pdf#anchor-1. Letöltés ideje: 2024. 08. 01.).

ÍTÉLETEK JEGYZÉKE

• CINIL Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI.
• C-625/19. PPU. sz. ügy Openbaar Ministerie kontra XD.
• NAIH-963-10/2022. 18-21.