# DATA-PROTECTION ANALYSIS OF BIOMETRIC SYSTEMS

# A BIOMETRIKUS RENDSZEREK ADATVÉDELMI SZEMPONTÚ ELEMZÉSE

KOVÁCS Tibor[1] – MIKLÓS Gellért[2]

**Abstract**

This article aims to provide a brief overview of the data protection considerations and requirements for the use of biometric data in different identification systems. The author illustrates the widespread use of biometric data in personal identification with international examples, as well as the regulatory requirements and potential dangers of this growing trend.

**Keywords**

biometrics, personal data, data protection, personal identification, GDPR, migration, border control

**Absztrakt**

Jelen cikk rövid áttekintést kíván nyújtani a biometrikus adatok különböző azonosító rendszerekben történő felhasználásának adatvédelmi megfontolásaival és követelményeivel kapcsolatban. A szerző nemzetközi példákkal illusztrálja a biometrikus adatok széleskörű felhasználási körét a személyazonosítás terén, ismertetve ennek az egyre növekvő trendnek a szabályozási követelményeit és lehetséges veszélyeit is.

**Kulcsszavak**

biometria, személyes adat, adatvédelem, személyazonosítás, GDPR, migráció, határellenőrzés

[1] kovacs.tibor@bgk.uni-obuda.hu | ORCID: 0000-0001-7609-9287 | associate professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi docens, tanszékvezető, Óbudai Egyetem Bánki Donát Gépész és Biztonság-technikai Mérnöki Kar

[2] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

## BEVEZETÉS

Az illegális határátlépés és a bevándorlás, a terrorizmus, a kiberbűnözés csak néhány olyan társadalmi feszültséget okozó jelenség napjainkban, amely fokozódó kihívás elé állítja a világ országait. Ez a növekvő nyomás és a biztonság iránti vágy egyben megteremti az igényt a megbízható, pontos és nem utolsó sorban költséghatékony személyazonosítás iránt.

A biometria, azaz egy élőlény – jellemzően ember – mérhető biológiai és viselkedési jegyeinek mérése és rögzítése, valamint az ezen alapuló azonosítás már régóta rendelkezésre áll. Az arc és hang alapján történő személyazonosítás egyidős az emberi civilizációval, a XIX. századtól kezdődően, a bűnüldöző hatóságok által rendszeresített ujjnyomat alapú azonosítás pedig széles körben elterjesztette a mérhető élettani tulajdonságok alapján történő azonosítás gyakorlatát. [1] Az élettani jellemzők felhasználhatók egy személy azonosítására és ellenőrzés céljából is. Személyazonosítás során az azonosítandó személy összevetésre kerül az adatállományban tárolt adatokkal, párosítva az egyező mintával és a hozzá társított adatokkal és jogosultságokkal (1:n típusú minta összehasonlítás). Ellenőrzés során a személy mért biológiai jellemzője összevetésre kerül a korábban már mért és a rendszerben tárolt mintával (1:1 típusú minta összehasonlítás). [2] A mérhető biológiai jellemzők köre a tudomány fejlődésével bővül, jelenleg a DNS, az arc és annak hőképe, a bőr mintázata, az ujjnyomat, ujjlenyomat vagy tenyérnyomat, a tenyér erezete vagy hőképe, a kéz geometriája, az írisz, a retina, míg a mért viselkedési jellemzők közül a kézírás, egy gomb vagy billentyű leütésének módja és sebessége, a beszédhang, valamint a járás módja a legjellemzőbben mért tulajdonságok.

A biológiai jellemzők egyik előnye, hogy azok rendszerint az azonosítandó személy tulajdonában vannak – mondhatni mindig kéznél vannak – és azok egy része huzamosabb ideig változatlanul lehetővé teszi a személy azonosítását. Ennek köszönhetően a biometrikus adatok széles körben felhasználásra kerülnek, legyen szó bűnüldözésről, vagy a határrendészet által rendszeresített biometrikus adatokat tartalmazó útiokmányokról. Napjainkban azonban a robbanásszerű technológiai fejlődés és a biztonság iránti növekvő igény megteremti a lehetőséget a korábbinál pontosabb azonosító eszközök, szenzorok költséghatékony létrehozására, a széleskörű mintavételre és azok tárolására, valamint a különböző biometrikus adatbázisok összekapcsolására.

A biometrikus azonosítás során, az élettani jellemzőkről készített sablonok és minták a hatályos adatvédelmi jogszabályok szerint személyes adatnak tekintendők, így az azonosítási eljárás kialakítása, valamint a minták kezelése során is érvényre kell jutnia az alkalmazandó alkotmányos és adatvédelmi jogi alapelveknek.

Az alábbiakban néhány tervezett, vagy már megvalósított biometrikus adatok felhasználására épülő személyazonosítás rendszer kerül bemutatásra, amelyek elemzése értékes tanulsággal szolgálhat a jövőben tervezett biometrikus adatbázisok vonatkozásában is.

## NEMZETKÖZI KITEKINTÉS

### Biometrikus SIM kártya regisztráció

A thai kormány 2017-től kötelezi a telekommunikációs szolgáltatókat, hogy SIM kártyák értékesítése során kötelezően rögzítsék az előfizetők ujjnyomatát vagy arcképét. A

biometrikus adatok az előfizető telefonszámához kapcsolódnak, majd az adatok egy központi nyilvántartásban kerülnek tárolásra, amelyet a Nemzeti Műsorszóró és Telekommunikációs Bizottság (National Broadcasting and Tele-communications Commission) felügyel. A regisztrációs kötelezettség egyaránt kiterjed az előfizetéses és a feltöltőkártyás SIM kártyákra is. A szolgáltatók a regisztrációs kötelezettségük elmulasztása esetén bírságra számíthatnak, szélsőséges esetben azonban az engedélyük is felfüggesztésre kerülhet. A szabályozás szigorításának indokául az elmúlt években elszaporodó terrorista merényletek szolgáltak. 2015-ben és 2016-ban is több olyan terrorista indíttatású merénylet történt Thaiföld forgalmasabb turista központjait célozva, amelyek során a pokolgépeket mobiltelefonokkal hozták működésbe. Az új, szigorúbb regisztrációs kötelezettségektől a thai kormány azt várja, hogy az megkönnyíti a korábbiakhoz hasonló terrorista cselekmények és egyéb bűncselekmény megakadályozását és felderítését is az által, hogy a bűncselekmény során felhasznált telefon tulajdonosa egyértelműen beazonosítható lesz a rendszerben tárolt adatok alapján. [3] A thaiföldi kezdeményezés csak egy, a világon számos más államban működő hasonló, biometrikus adatokon alapuló regisztrációs rendszerhez képest. Pakisztán és Banglades már 2015-ben bevezette az ujjnyomaton alapuló SIM kártya regisztrációt, míg Nigériában 2011 óta működik hasonló rendszer.

A kritikusok szerint azonban a thaihoz hasonló kötelező, biometrikus adatok rögzítésére alapuló regisztrációs rendszerek súlyosan korlátozzák az érintettek magánélethez való jogát, valamint nem váltják be a hozzájuk fűzött reményeket a terrorizmus ellen folytatott harc során. Egyrészt a SIM kártya kötelező regisztrációja megszünteti az anonim, névtelen kommunikáció lehetőségét az érintettek számára, míg az állam számára lehetővé teszi az érintettek helyének és személyazonosságának pontos meghatározását. Egy biometrikus adatokat, telefonszámot és helymeghatározási adatokat is tartalmazó nyilvántartás könnyen visszaélésekhez vezethet, vagy lehetővé teheti az érintettekkel kapcsolatos profilalkotást is. A névtelenség ugyan valóban megnehezítheti a bűncselekmények felderítését, azonban az újságírok, emberi jogi aktivisták, vagy más sérülékeny közösségek tagjai számára egy eszköz is, amely lehetővé teszi, hogy gyakorolják a szólásszabadsághoz fűződő jogukat. Könnyen belátható, hogy egy ilyen rendszer nagymértékben kiszolgáltatottá teszi ezeket a csoportokat, különösképpen, ha a rendszerrel szemben kritikus hangon szólalnak meg. [4] A tapasztalatok alapján hátránya továbbá a kötelező regisztráción alapuló rendszereknek, hogy hatásukra megnő a kereslet a nem regisztrált, vagy fals személyiséggel regisztrált SIM kártyák iránt, amely igényt a feketepiac siet kielégíteni. Ezzel összefüggésben megnő a személyiség lopások, valamint a már regisztrált eszközök ellen elkövetett lopások száma is. Nincs azonban kimutatható össze-függés azon bűncselekmények számával, amelyekre hivatkozással a kormányok indokolták a regisztráció bevezetését. Erre a tanulságra jutott mind a Pakisztánban, mind a Mexikóban bevezetett hasonló rendszer elemzése kapcsán a telekommunikációs szolgáltatókat tömörítő GSMA szervezet is. [5]

A fentiek alapján javasolta 2015-ben az ENSZ szólásszabadságért felelős különleges előadója vizsgálata eredményeként, hogy az államok tartózkodjanak attól a gyakorlattól, hogy a digitális kommunikációhoz és az online szolgáltatásokhoz való hozzáférést a felhasználók azonosításához kössék és a mobil felhasználók számára a SIM-kártya kötelező regisztrációját követeljék meg. [6]

## Az indiai Aadhaar rendszer

Napjainkban hatalmas problémát jelent a világ számos részén, hogy a lakosság egy jelentős része – főleg a vidéki, nehezen megközelíthető, gyéren lakott területeken – nem rendelkezik semmilyen személyazonosító dokumentummal. Különösen igaz ez a szubszaharai Afrikára és Ázsia egyes részeire. Ezek a személyazonosító okmányokkal nem rendelkező emberek sok szempontból láthatatlanok a kormányok számára és a megfelelő dokumentumok hiányában a társadalmi ellátórendszeren kívül rekednek. További nehézséget jelent a fejlődő világ országaiban a társadalmi juttatásokkal kapcsolatos korrupció, valamint azok nem hatékony elosztása. Az indai kormány becslése szerint a legszegényebb társadalmi csoportok számára biztosított rizs támogatás 15%-a, a búza támogatás 54%-a, míg a cukor támogatás 48%-a veszett el a korrupció és a nem hatékony elosztás következtében. [7] Indiában az ezredforduló környékén kezdődött meg a párbeszéd egy új nemzeti személyazonosítási rendszer szükségességéről és annak megvalósításáról. Az új rendszer a tervek szerint erősítette volna a nemzetbiztonságot (főleg a személyek egyértelmű azonosítása által a vitatott hovatartozású és kevert etnikumú területeken), valamint megszüntette volna a fennálló személyazonosítási rendszerhez kapcsolódó hamis személyazonosságokat.

Az Aadhaar névre keresztelt biometrikus adatokon alapuló személyazonosító rendszer 2010-es indulása óta hatalmas fejlődésen ment keresztül. Jelenleg 1,2 milliárd ember rendelkezik Aadhaar azonosítóval, amely a világ össznépességének 16%-a. A rendszer egy tizenkét számjegyből álló személyi azonosító számra épül, amelyet elektronikusan és plasztik kártyán is megküldenek a regisztrálók számára. A rendszer célja kettős, egyrészt megbízhatóan azonosítani a számsor birtokosát és csökkenteni az azonosítással összefüggő hibákat, másrészt pedig biztosítani, hogy a különböző kormányzati támogatásokat csak az arra jogosultak vehessék igénybe.

A regisztráció nincs nemzetiséghez kötve, bámely indiai lakos jogosult Aadhaar azonosítót létrehozni, ehhez elég bemennie a legközelebbi felvételi központba és megadni a szükséges adatait. Az azonosító létrehozásához szükséges a név, születési idő, a nem, valamint a lakcím megadása, valamint egy arcképet ábrázoló fénykép. A telefonszám és az email cím megadása opcionális, azonban számos szolgáltatás igénybevételének feltétele. A fentieken túlmenően a regisztráció során mind a tíz ujjról mintát készítenek. Ennek oka, hogy Indiában a lakosság jelentős része mezőgazdasági és ipari munkából tartja fent magát és családját, így gyakran előfordul, hogy az ujjak barázdái a kétkezi munkától kopnak, ezáltal meg-nehezítve vagy ellehetetlenítve a pontos azonosítást. Erre tekintettel az ujjnyomat mellett a személyek mindkét íriszéről is mintát vesznek. A minták és a felvett adatok titkosításra, majd továbbításra kerülnek a Központi Személyes Adat Nyilvántartásba (Central Identities Data Repository). Ott a beérkezett adatok összevetésre kerülnek a rendszerben tárolt többi adattal, hogy kiszűrjék a duplikációkat vagy egyéb hibákat. Ezt az ellenőrzést egy ügyintéző felügyeli, így egyetlen jelentkező regisztrációját sem utasíthatja el automatikusan a rendszer emberi felülvizsgálat nélkül. Ezt követően kerül generálásra a véletlenszerű tizenkét számjegyből álló Aadhaar számsor, amely önmagában nem hordoz információt a tulajdonosáról. Abból nem lehet következtetéseket levonni, ellentétben számos más személyazonosításra használt számmal, mint amilyen a magyar lakcímkártyákon szereplő személyi szám is. A rendszer használata 2016-tól kötelező feltétele a kormányzati támogatások és segélyek igénybevételének. Az indiai kormány állítása szerint a rendszer a regiszt-

rált tagok számának növekedésével párhuzamosan eredményez évről évre egyre több megtakarítást az állam számára. Ezzel párhuzamosan számos szolgáltató, köztük bankok és telekommunikációs cégek is Aadhaar azonosításhoz kötötték szolgáltatásuk nyújtását.

Az Aadhaar rendszer öt módon teszi lehetővé a személyek azonosítását. Egyrészt a szolgáltatók vagy a támogatást folyósító intézmények összevethetik a rendszerben tárolt adatokat a személy által megadott és igazolt személyi adatokkal, másrészt amennyiben a személy a regisztráció során megadott telefonszámot vagy email címet, úgy a rendszer arra egyszer használatos jelszót küldhet az azonosítás céljából. Az azonosítás további módja az ujjnyomat vagy az írisz vagy mindkét biometrikus jellemző rendszerben tárolt mintával való összevetése, valamint kétfaktoros hitelesítés, amely során a biometrikus azonosításon túl egy egyszer használatos jelszó is megküldésre kerül a megadott elérhetőségek valamelyikére. Az azonosítás során a rendszer az igényeknek megfelelően kétféle visszajelzésre képes. Az egyik egy igen/nem típusú azonosítás, amely során az ellenőrizendő személy adatai kerülnek összevetésre a rendszerben tárolt adatokkal. A másik egy „ismerd meg az ügyfeled" („know your customer" vagy „KYC") jellegű azonosítás, amely sikeres azonosítás esetén a szolgáltató rendelkezésre bocsátja a személy személyazonosító adatait is. [8]

Egy ilyen hatalmas, biometrikus adatokon alapuló rendszernek robosztus információbiztonsági követelményeknek kell megfelelnie az esetleges adatszivárgások, adatlopások és egyéb incidensek megakadályozása érdekében, máskülönben megrendülhet az emberek rendszerbe vetett bizalma. Az Aadhaar rendszer fejlődését is számos botrány, valamint bírósági ítélet kísérte és szorosan összefonódott az adatvédelemi jog és a személyes adatok védelmének indiai fejlődésével. A rendszer megalkotásának idején Indiában nem volt önálló adatvédelmi törvény, amely az Aadhaar rendszerhez kapcsolódó adatkezelés és adattovábbítást szabályozta volna. 2017-ben a Puttaswamy kontra India ügyben az indiai legfelsőbb bíróság az Aadhaar rendszer vizsgálatával kapcsolatban megállapította, hogy az indiai alkotmány 21 cikke alapján a magánélethez való jog egy alkotmányosan védett alapjog. A döntés mérföldkőnek számított a magánélethez való jog indiai értelmezésében, valamint egy egységes adatvédelmi jogszabály megalkotásának folyamatában, amely feltehetőleg továbbgyűrűző hatást fog gyakorolni az alapvető jogok és személyes szabadságok indiai rendszerére. [9] 2018-ban egy francia információbiztonsági szakértő arról számolt be, hogy több mint húszezer nyilvánosan hozzáférhető Aadhaar számhoz kapcsolódó adatot tárt fel a hozzájuk tartozó bankszámla adatokkal különböző kormányzati honlapokon. [10] Más esetekben újságírók arról számoltak be, hogy bizonyos összegekért hozzáférhettek volna több ezer, vagy esetenként több millió Aadhaar számhoz, valamint a hozzájuk kapcsolódó személyes adatokhoz is. [7] További probléma a regisztráció elhúzódása, amely közvetetten több ember halálát is okozhatta, ugyanis a sikeres regisztrációt megelőzően nem folyósítható az igénylők számára a kormányzati segély. Az elhúzódó regisztráció azonban szélsőséges esetben több hónapig is eltarthat, amely időtartam alatt az igénylők segély nélkül maradnak. Számos esetben számoltak be az Aadhaar azonosítóhoz kapcsolódó személyiséglopásról is, amelynek során a bűnözők más személyek Aadhaar azonosítójával vettek igénybe szolgáltatásokat vagy követtek el visszaéléseket, amelyekkel szemben az áldozatok és a hatóságok gyakorlatilag tehetetlenek. Az áldozatok számára a profiljuk törlését javasolja az Aadhaar rendszer üzemeltetője, azonban ezzel együtt elveszítenék hozzáférésüket számos szolgálatáshoz, segélyhez is. [11]

**EU igazságügyi, bűnüldözési és határőrizeti rendszereinek összekapcsolásáról szóló interoperabilitási rendeletek**

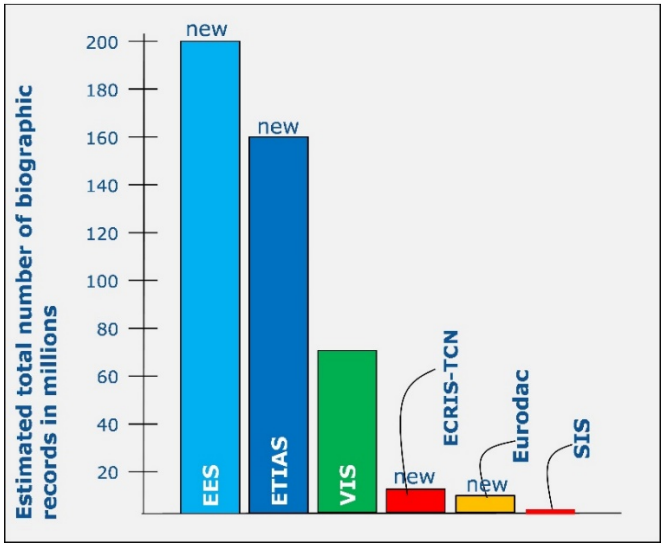
Az Európai Unió külső határaira nehezedő migrációs nyomásra válaszul, valamint a belső biztonság fokozása érdekében mind az Európai Parlament, mind az Európai Bizottság jogalkotási programjában szorgalmazta a már létező határőrizeti és bűnüldözési rendszerek fejlesztését, valamint új rendszerek megalkotását. A hatékonyságnövelés egyik módja a már meglévő rendszerek interoperabilitásának, azaz együttműködésre való képességének megteremtése. Ezáltal a korábban különálló adatbázisok összekapcsolásra kerülnek és a bennük tárolt adatok egyetlen kereséssel elérhetővé válnak az arra feljogosított szervek és személyek számára, ezzel időt és erőforrásokat megtakarítva. Több korábbi felmérés és hatásvizsgálat is megállapította, hogy a nem megfelelő mennyiségű, fajtájú és megbízhatóságú adat megnehezíti a személyiség elleni csalások elleni eredményes küzdelmet. Hosszas előkészítés után 2019. május 20-án fogadta el az interoperabilitás kereteinek megállapításáról szóló 2019/817, valamint 2019/818 számú rendeleteket az Európai Unió (a továbbiakban rendeletek). A két rendeletet együtt kell olvasni, azok felépítése, logikája, megegyezik. A fenti két rendelet mellett kidolgozásra és elfogadásra kerültek azok a további jogi aktusok, amelyek megteremtik az interoperabilitáshoz szükséges keretrendszert. Az interoperabilitás megteremtése érdekében 2019. június 11-én hatályba lépett az Európai Parlament és a Tanács 2019/816 rendelete, amely a harmadik országbeli állampolgárok és a hontalan személyekkel szemben hozott ítéletekre vonatkozó információval egészíti ki az Európai Bűnügyi Nyilvántartási Információs Rendszert (ECRIS-TCN), 2017 decemberében lépett hatályba a tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról szóló 2017/2226 EU rendelet, biztosítva az összekapcsolhatóságát a vízuminformációs rendszerrel (VIS). Az ujjlenyomatok összehasonlítását szolgáló EURODAC rendszer (603/2013/EU rendelet) felülvizsgálatáról szóló döntés jelenleg az Európai Parlament első olvasatára vár. Az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásra került 2018. októberében a 2018/1240 EU rendelet által. Az ETIAS olyan harmadik országbeli állampolgárokra vonatkozóan került megalkotásra, akik mentességet élveznek a vízumkötelezettség alól. Részükre bevezetésre kerül az utazási engedély, valamint meghatározásra kerülnek az annak kiadására, illetve megtagadására vonatkozó feltételek és eljárások. Megvalósult a Schengeni Információs Rendszer (SIS) alkalmazásának kiterjesztése a jogellenesen tartózkodó harmadik országbeli állampolgárok visszaküldése céljából a 2018 decembere óta hatályos 2018/1860 rendelet által és végezetül 2018 decembere óta hatályos a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai uniós ügynökségről szóló (eu-LISA) 2018/1726 EU rendelet.

Amint az az előzőekből is látszik, az interoperabilitás megteremtése egy összetett, több lépcsőből álló jogszabályalkotási folyamat eredménye. A folyamat eredményeként létrehozásra kerül:

- az európai keresőportál („european search portal" vagy „ESP"), amely lehetővé teszi az összes vonatkozó információs rendszer egyidejű keresését és az összes ellenőrzés eredményének egyetlen számítógépes képernyőn történő elérését. A portál nem tárol vagy dolgoz fel új adatokat, és nem változtatja meg a felhasználók hozzáférési jogait;

- a közös biometrikus megfeleltetési szolgáltatás („shared biometric matching service”, a továbbiakban: közös BMS), amely lehetővé teszi a biometrikus adatok (ujjlenyomatok és arcképek) lekérdezését és összehasonlítását a fentebb felsorolt központi rendszerekből (SIS, az Eurodac, VIS, az EES és az ECRIS-TCN);
- a közös személyazonosítóadattár („common identity repository”, a továbbiakban: CIR), amely tárolná az Eurodac-ban, a VIS-ben, az EES-ben, az ETIAS-ban és az ECRIS-TCN-ben rögzített harmadik országbeli állampolgárokkal kapcsolatos alapvető személyi adatokat (név, születési hely és idő) és biometrikus adatokat, lehetővé téve a hatékony személyazonosság ellenőrzést az EU tagállamai területén,
- a többszörös személyazonosságot felismerő rendszer („multiple-identity detector”, a továbbiakban: MID), amely lehetővé tenné a személyek helyes személyazonosságának felderítését, valamint a személyiségcsalások és többszörös személyazonosságok felderítését.

A rendeletek egy kétlépcsős adatbetekintési megközelítést alkalmaznak a CIR-ben történő keresés esetén. A kétlépcsős adatbetekintés során a naplóknak tartalmazniuk kell a nyomozás vagy az ügy nemzeti aktájára való hivatkozást, ami azt jelzi, hogy a lekérdezést terrorista bűncselekmények vagy egyéb súlyos bűncselekmények megelőzése, felderítése vagy nyomozása céljából kezdeményezték, valamint a lekérdezések célját is. A kétlépcsős adatbetekintés során a keresett személlyel kapcsolatos lekérdezés során először csak egy egyezés megjelölés típusú válasz jelenik meg, amely arra utal, hogy az adat szerepel az EES-ben, a VIS-ben, az ETIAS-ban vagy az Eurodacban. A kétlépcsős adatbetekintés már önmagában adatkezelésnek minősül, ugyanis már a keresett személyre vonatkozó igen/nem találat és az abból levonható következtetések (tehát, hogy a keresett személy megtalálható valamelyik adatbázisban) személyes adatnak minősül. Az új rendszer a becslések szerint 2021-ig 218 millió harmadik országbeli személy személyazonosító és biometrikus adatait tartalmazná. [12]




*1. Ábra: A rendszerek által kezelt biometrikus adatok becsült száma millióban. Forrás: Európai Bizottság, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0473&from=EN*

Az adatbázisban tárolandó adatok mennyiségének nagysága és jellege miatt egy esetleges adatvédelmi incidens súlyos károkat okozhatna sok személy számára. Amennyiben ezek a személyes adatok rossz kezekbe kerülnének, az adatbázis veszélyes eszközzé válhat az alapvető jogok ellen. Erre tekintettel fogalmazott úgy a rendeletekhez fűzött véleményében az Európai Adatvédelmi Biztos, hogy a rendeletek által létrehozott központosított adatbázis egy olyan pont, ahonnan nincs visszatérés. [13] A rendeletek egy olyan komplex rendszert hoznak létre, amelyre egyaránt vonatkozik az általános adatvédelmi rendelet (2016/679 EU rendelet), a bűnügyi adatvédelmi irányelv (2016/680 EU irányelv), az azt nemzeti jogba átültető jogszabályok, valamint a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról szóló 2018/1725 EU rendelet. A rendeletek szövegükben nevesítik is ezen jogszabályokat, azonban azt már nem határozzák meg, hogy pontosan mely adatkezelési műveletekre mely jogszabály rendelkezései az irányadók.

Az interoperabilitási rendeletek megalkotásának folyamatban szakértőként mind az Európai Adatvédelmi Biztos (EDPS), mind a 29. cikk alapján létrehozott Adatvédelmi Munkacsoport is részt vett és azt számos kritikával illette. Állásfoglalásában az Európai Adatvédelmi Biztos rámutatott, hogy amint arra a rendeletek 40. preambulumbekezdése is utal, az érintett személyek pontos azonosítása céljából végzett adatkezelési műveletek az Európai Alapjogi Charta 7. és 8. cikke által védett alapvető jogaikba való beavatkozásnak minősül, ezért ezeket az új adatkezelési műveleteket a Charta 52. cikk (2) bekezdés alapján alá kell vetni a szükségesség arányosság tesztnek. Ennek során kiemelt jelentősége van az adatkezelések szükségességét alátámasztó, kellően konkrétan megfogalmazott indokra és az azt alátámasztó bizonyítékokra. A rendeletek indokolása ugyan megnevezi a többes személyazonosságok, a személyazonosság csalások, valamint a terrorizmus elleni küzdelmet, azonban elmulasztja számszerűsíteni a hivatkozott jelenségek mértékét, amely megnehezíti a teszt elvégzését. Önmagában az „illegális migráció elleni küzdelem és a biztonság magas szintjének biztosítása" túl tág megfogalmazás és ezen nem változtat az sem, az uniós jogszabály a rendelkezés további megfogalmazását a tagállami jogalkotásra bízza, mint ahogyan a rendeletek 20. cikke teszi. Ez semmiképpen sem felel meg az Európai Unió Bírósága (CJEU) által a Digital Right Ireland ügyben lefektetett korlátozottság és pontosan körülhatároltság követelményeinek.

Az Európai Adatvédelmi Biztos felhívta továbbá a figyelmet a beépített és alapértelmezett adatvédelem elvének alkalmazására a rendszer tervezése és kialakítása során és annak alapján a megfelelő adatvédelmi biztosítékok beépítését. [13] Mind az Európai Adatvédelmi Biztos, mind a 29. cikk szerinti munkacsoport felhívta továbbá a figyelmet arra, hogy adatbiztonsági szempontból egy központosított adatbázis létrehozása növeli a visszaélés és az adatok jogellenes felhasználásának, valamint az eredeti funkción való túlterjeszkedés („function creep") kockázatát. [14] Tekintettel arra, hogy az adatbázisokhoz a tagállamok rendvédelmi és határvédelmi szervei is hozzáféréssel fognak rendelkezni, a hozzáférési pontok száma ezzel több ezerre lesz tehető, amely súlyos biztonsági kockázatot jelent. Ennek ellenére a rendeletek 42. cikke csak a rendszereket kifejlesztő és irányító eu-Lisa számára fogalmaz meg konkrét adatbiztonsági előírásokat, míg tagállamok, az Europol és az ETIAS központi egysége részére csak azokkal egyenértékű intézkedések meghozatalát

írja elő. Ez a megfogalmazás azonban könnyen eltérő szintű adatbiztonsági intézkedések gyakorlati megvalósításához vezethet.

## ADATVÉDELMI MEGFONTOLÁSOK

A magyar adatvédelmi jog, valamint az Európai Unió általános adatvédelmi rendelete alapján személyes adatnak minősül az azonosított vagy azonosítható személyre vonatkozó bármely információ. Ebből kifolyólag, mind a biometrikus adat, mind az abból leképzett sablonok kezelésének meg kell felelnie az adatvédelmi jog által meghatározott elveknek és előírásoknak. A biometrikus adatok az általános adatvédelmi rendelet alapján a személyes adatok különleges kategóriájába tartoznak és kezelésükre további szabályok vonatkoznak. A biometrikus adatok kezelése csak abban az esetben jogszerű, amennyiben az adatkezelés rendelkezik egy 6. cikk szerinti jogalappal és attól függetlenül azonosításra és megjelölésre kerül legalább egy, a 9. cikk (2) bekezdésében felsorolt valamely speciális feltétel is. A 6. cikk szerinti választott jogalapnak és a 9. cikk szerinti speciális esetkörnek nem kell egymással összefüggésben állnia. [15]

A biometrikus adatok fokozott védelmének indoka az, hogy a biometrikus adatok közvetlenül kapcsolódnak az érintetthez, csak rájuk jellemzőek és állandók, ezért nem, vagy csak nehezen változtathatók meg, nem tagadhatók le, ezért visszavonhatatlanok. [16] Éppen ezért a biometrikus adatokkal kapcsolatos bármely jogsértés veszélyezteti a biometrikus adat további felhasználását és felhasználhatóságát, amelyekre vonatkozóan nincs lehetőség a jogsértés következményeinek enyhítésére.

Az Európai Unió Alapjogi Chartájának 8. (1) bekezdése kimondja, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez. A személyes adatokat csak az érintett személy hozzájárulása vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Az 52. cikk (1) bekezdése azonban rögzíti, hogy a Chartában elismert jogok és szabadságok gyakorlása csak a törvény által, és a jogok lényeges tartalmának tiszteletben tartásával korlátozhatók. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

Magyarország Alaptörvénye szintén védelemben részesíti a személyes adatokat. Az alaptörvény VI. (3) bekezdése alapján, mindenkinek joga van személyes adatai védelméhez. A személyes adatok védelméhez fűződő jog tehát alkotmányos alapjog. Magyarország alkotmányos hagyományai, valamint az Alkotmánybíróság töretlen gyakorlata és az Alaptörvény jelenleg is hatályos rendelkezése alapján 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. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) számos állásfoglalásában következetesen képviselte azt az álláspontot, hogy a biometrikus adatok kezelése során érvényesülnie kell a szükségesség és arányosság elvének. Egy alkotmányjogi panasszal kapcsolatos ügy során elkészített szakértői véleményében a NAIH hivatkozással az Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport biometrikus technológiák terén történt fejleményekről szóló 3/2012. számú véleményére (WP193), kifejti, hogy a biometrikus rendszerek alkalmazása felveti az arányosság kérdését a feldolgozott adatok

tekintetében. Mivel a biometrikus adatok csak akkor kezelhetők, ha megfelelőek, relevánsak és nem túlzott mértékűek, ezért minden esetben mérlegelni kell a kezelt adatok szükségességét, arányosságát, valamint azt, hogy az adatkezelés által elérni kívánt cél megvalósítható lenne-e a magánszférát kevésbé korlátozó módon. Ezért egy biomerikus rendszer arányosságának elemzése során „előzetesen mérlegelni kell, hogy a rendszer szükséges-e a meghatározott igény kielégítéséhez, azaz használata elengedhetetlen-e ehhez, vagy inkább annak legkényelmesebb vagy legköltséghatékonyabb módja. Egy második megfontolandó tényező az, hogy a rendszer valószínűleg elég hatékony lesz-e az adott igény kielégítésében, tekintettel a használni tervezett biometrikus technológia sajátos jellemzőire. A harmadik mérlegelendő szempont, hogy arányos-e az elvárt előnyökkel, ha a rendszer miatt sérül a magánélet védelme. Ha az előnyök viszonylag kisebbek, például kényelmesebb az eljárás vagy kismértékű költségmegtakarítás érhető el, akkor nem helyénvaló, ha sérül a magánélet védelme. Egy biometrikus rendszer megfelelőségének értékelése során a negyedik szempont annak megfontolása, hogy a magánéletbe kisebb mértékben beavatkozó módszerek elérhetnék-e a kívánt célt" [17] Abban az esetben, ha a kívánt cél más, a magánéletbe kisebb mértékben beavatkozó módszerrel is elérhető, úgy az adatkezelőnek annak megvalósítására kell törekednie.

A biometrikus adatok kezelésének a fentieken túlmenően természetesen meg kell felelnie a személyes adatok kezelésére vonatkozó elveknek és előírásoknak. Így az adatkezelésnek, jogszerűnek, tisztességesnek, valamint az érintettek számára átláthatónak kell lennie. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet és azoknak az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk. A kezelt biometrikus adatoknak továbbá pontosnak és szükség esetén naprakésznek kell lenniük, a pontatlan személyes adatokat pedig törölni, vagy helyesbíteni kell.

## KÖVETKEZTETÉSEK

A fenti példákon keresztül megállapítható, hogy a biometrikus adatok rendkívül sokoldalúan felhasználhatók személyazonosítás céljából. Kijelenthető, hogy a technológiai fejlődés eredményeképp már csak a politikai akarat és a jogszabályi környezet határozza meg a biometrikus azonosításra épülő rendszerek korlátait. Az indiai Aadhaar rendszer például pozitív példája annak, hogy hogyan lehet a világ legnépesebb működő demokráciájában viszonylag rövid idő alatt bevezetni egy ilyen személyazonosító rendszert, valamint, hogy egy ilyen rendszer és az azzal járó digitális megoldások milyen járulékos előnyökkel járnak az azt kiépítők számára. Indiában a felmérések szerint csökkent a kormányzati segélyekhez kapcsolódó csalások száma és ezáltal a költségvetésre nehezedő teher is, ami lehetővé tette a tényleges rászorulóknak járó összegek folyamatos emelését is. Azonban ugyan ilyen fontos a negatív tapasztalatok, példák elemzése is. A személyes adatok – köztük a biometrikus adatok – nem megfelelő védelme fizikai, vagyoni vagy nem vagyoni károkhoz vezethet a rendszerben tárolt személyek számára.

Amint az a biometrikus azonosításhoz kötött SIM kártya regisztráció kapcsán is ismertetésre került, a biometrikus azonosítás nem minden esetben éri el önmagában a kitűzött célt. A személyazonosítás megnövelt pontossága pedig nem minden esetben felel meg a szükségesség arányosság követelményének. Mivel a magánélethez és a személyes adatok védelméhez fűződő jog a legtöbb államban nemzetközi szerződések és az alkotmány által

védett alapvető jog, így a biomterikus adatok kezelése esetén szükségszerű ennek a tesztnek az elvégzése. Különösképp igaz ez az Európai Unió intézményeire és annak tagállamaira, köztük Magyarországra. A NAIH gyakorlatában következetesen érvényre juttatta a biometrikus adatok fokozottabb védelmét és számos esetben írta elő adatkezelők számára a biometrikus azonosítás helyett (NAIH-6300-2/2012/V.) más, a személyhez fűződő jogokat kevésbé korlátozó módszerek alkalmazását.

Már ma is számos olyan személyazonosító szolgáltatás vehető igénybe a fogyasztók számára, amely biometrikus adatok felhasználására épül. Ilyenek például az okostelefonokba vagy laptopokba épített kapacitív ujj-nyomat érzékelők. Ezen szolgáltatások a legtöbb esetben azonban nem kötelezőek a fogyasztók számára, akik az általános adatvédelmi rendelet alapján kifejezett hozzájárulásukkal felhatalmazhatják a szolgáltatókat ezen adatok kezelésére. Más a helyzet azonban olyan esetekben, amikor az adatkezelő és az érintettek között aszimmetrikus viszony van. Ilyen lehet egy munkáltató és a munkavállaló, vagy az állam és az állampolgárok viszonya. Ezekben az esetekben fokozottan érvényesül a szükségesség és arányosság, hiszen a kifejezett hozzájárulás, mint jogosító körülmény az aszimmetrikus viszonyra tekintettel nem lehet jogszerű. Ebből adódóan például munkahelyi körülmények között csak kifejezetten indokolt esetben ad teret az adatvédelmi hatóság a kötelező biometrikus azonosításnak, mint például egy gyógyszeripari kutató laborítórium, ahol vírusokat is tárolnak, vagy egy erőmű.

Az általános adatvédelmi rendelet alapján, a biometrikus adatok kezelhetők jelentős közérdekre történő hivatkozással is, amennyiben az azt előíró uniós jog vagy tagállami jog arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő. A világon megfigyelhető általános jelenség, hogy a közterületeket egyre több, egyre jobb minőségű képet készítő, arcfelismerésre is képes kamera figyeli meg, amelyek másként pótolhatatlan segítséget nyújtanak a bűnüldöző szerveztek részére a bűncselekmények felderítése során. Ezek a kamerák azonban alkalmasak arra is, hogy az állam megfigyelje állampolgárait. Fokozottan igaz ez a biometrikus azonosítók kezelése esetén. Amint arra véleményében mind a NAIH, mind az Európai Adatvédelmi Biztos és a 29. cikk szerinti Adatvédelmi Munkacsoport kitért, a biometrikus azonosítók elválaszthatatlanok az érintettektől, így azok elvesztése, kompromittálódása visszafordíthatatlan következményekkel járhat az érintettek számára. Erre tekintettel nevezte az Európai Adatvédelmi Biztos a különböző Európai Uniós határvédelmi, bűnüldözési és igazságszolgáltatási rendszereinek összekapcsolását egy olyan pontnak, ahonnan nincs visszatérés. Mind a jelenlegi, mind a jövőben megalkotandó biometrikus adatbázisok felé elvárás az, hogy létrehozásuk indoka, kellőképpen konkrétan és megfelelően alátámasztottan igazolásra kerüljön. Egy homályosan, vagy túl általánosan megfogalmazott indok, egy jövőbeli fenyegetésre való hivatkozás könnyen a célhoz kötött adatkezelés és a készletező adatgyűjtés tilalmába ütközhet. A bűnügyi nyilvántartás jelenleg is tartalmaz biometrikus adatokat Magyarországon. A nyilvántartást szabályozó törvény azonban részletesen szabályozza a nyilvántartott biometrikus adatok körét, valamint felhasználásuk célját, megőrzésük idejét és részletesen szabályozza az érintetteket megillető jogokat, valamint az őket védő garanciális szabályokat.

Az Európai Unió tagállamai közül Franciaország kívánja először bevezetni az arcfelismerésre és biometrikus adatokra épülő széleskörű személyazonosítási rendszert (Alicem), azonban a francia adatvédelmi hatóság (CNIL) már jelezte a jogalkotó számára fenntartásait a tervezettel kapcsolatban, ugyanis álláspontja szerint annak megvalósítása uniós jogba ütközik és nemzetközi kötelezettségekbe ütközik. Amennyiben más uniós tagállamok is hasonló rendszer bevezetését terveznék, úgy feltehetőleg a nemzeti adatvédelmi hatóságok ott is hasonló következtetésre jutnának. Ennek oka, hogy az Európai Unió tagállamaira vonatkozó nemzetközi szerződések, uniós jogszabályok és nemzeti jogszabályok olyan komplex rend-szert alkotnak, amelyek jelentősen behatárolják ezeknek a rendszereknek a megvalósíthatóságát, valamint meghatározzák az érvényesítendő elveket és garanciákat is. Máig ható elvi éllel jelentette ki például a magyar Alkotmánybíróság, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása alkotmányellenes, mert az az érintetett az adatkezelővel szemben kiszolgáltatottá teszi, egyenlőtlen helyzetet teremtve ezzel. Erre tekintettel egy olyan általános személyazonosító rendszer, amely a lakosság minden tagjára kiterjedően tartalmazza az érintettek biometrikus adatait egyelőre nem valószínű Magyarországon.

## FELHASZNÁLT FORRÁSOK

[1] BALLA J. „Biometrikus adatok a személyazonosításban” megjelent „A változó rendészet aktuális kihívásai” című konferenciakötetben, Pécs, 2013. pp. 287-294

[2] KOVÁCS T., MILÁK I., OTTI CS. „A biztonságtudomány biometriai aspektusai” megjelent „A biztonság rendészettudományi dimenziói – változások és hatások” című konferenciakötetben, Pécs, 2012. pp. 485-496

[3] “Thailand to require biometric registration for SIM cards” [Online]. Elérhető: https://asia.nikkei.com/Politics/Thailand-to-require-biometric-registration-for-SIM-cards [Hozzáférés dátuma: 2021 március 12.].

[4] “101: SIM Card Registration” [Online]. Elérhető: https://privacyinternational.org/explainer/2654/101-sim-card-registration [Hozzáférés dátuma: 2021 március 12.].

[5] “Mandatory registration of prepaid SIM cards - Addressing challenges through best practice” [Online]. Elérhető: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf [Hozzáférés dátuma: 2021 március 12.].

[6] “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” [Online]. Elérhető: https://www.undocs.org/A/HRC/29/32 [Hozzáférés dátuma: 2021 március 12.].

[7] „Lessons from Aadhaar: Analog aspects of digital governance shouldn’t be overlooked” [Online]. Elérhető: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/lessons_from_aadhaar.pdf [Hozzáférés dátuma: 2021 március 12.].

[8] https://uidai.gov.in/ecosystem/authentication-ecosystem/operation-model.html [Online] [Hozzáférés dátuma: 2021 március 12.].

[9] https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/ [Online] [Hozzáférés dátuma: 2021 március 12.].

[10] https://timesofindia.indiatimes.com/business/india-business/vigilante-hacker-flags-security-concerns-in-aadhaar-govt-websites-again/articleshow/63298630.cms [Online] [Hozzáférés dátuma: 2021 március 12.].

[11] https://www.moneylife.in/article/aadhaar-nightmares-coming-true-how-ameya-dhapre-is-enduring-living-hell-with-his-aadhaar-report/59034.html [Online] [Hozzáférés dátuma: 2021 március 12.].

[12] „Document 52017SC0473 - Az interoperabilitási rendeleteket kísérő hatástanulmány" [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019R0818&from=EN [Hozzáférés dátuma: 2021 március 12.].

[13] „Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems" [Online]. Elérhető: https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf [Hozzáférés dátuma: 2021 március 12.].

[14] „Opinion on Commission proposals on establishing a framework for interoperability - wp266" [Online]. Elérhető: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198 [Hozzáférés dátuma: 2021 március 12.].

[15] Miklós G., Kovács T. „A biometrikus adatok kezelésének jogi szabályozása," Hadmérnök, XIV. kötet 1. szám, 2019., Elérhető: http://www.hadmer-nok.hu/191_01_miklos.pdf

[16] http://public.mkab.hu/dev/dontesek.nsf/0/99aeb34aebaa6c68c1257dda005de077/$FILE/IV_6_7_2015_NAIH_allasfoglalas.pdf [Online] [Hozzáférés dátuma: 2021 március 12.].

[17] „3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről" [Online]. Elérhető: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf [Hozzáférés dátuma: 2021 március 12.].

[18] Berek L., Berek T., Berek L., Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.