HADMÉRNÖK

XIV. Évfolyam 1. szám – 2019. március 10.32567/hm.2019.1.1

A BIOMETRIKUS ADATOK KEZELÉSÉNEK JOGI SZABÁLYOZÁSA

LEGAL REGULATION OF THE PROCESSING OF BIOMETRIC DATA

KOVÁCS Tibor; MIKLÓS Gellért

(ORCID: 0000-0001-7609-9287); (ORCID: 0000-0002-3757-6834)

miklos.gellert@phd.uni-obuda.hu; kovacs.tibor@bgk.uni-obuda.hu

Absztrakt

Jelen cikk rövid áttekintést kíván nyújtani a biometrikus adatok felhasználásáraa felhasználására és a biometrikus azonosítás során végrehajtott adatkezelésekre vonatkozó jogszabályi környezetről és az alkalmazandó magyar és európai uniós (EU) jogszabályokról. Bemutatásra kerülnek a biometrikus azonosítási eljárások működési elvei, a biometrikus adatok kezelésére vonatkozó releváns jogszabályok, valamint a Nemzeti Adavétdelmi és Információszabadság Hatóság és a 29-es cikk szerint létrehozott Adatvédelmi Munkacsoport (WP29) témához kapcsolódó véleményei, iránymutatásai és állásfoglalásai.

Kulcsszavak: *biometrikus azonosítás, biometrikus adat, adatvédelem*

Abstract

The present article aims to provide a brief overview of the legal environment for data processing in biometric authentication and the applicable Hungarian and European Union (EU) legislation. Presenting the principles of biometric authentication, the relevant legislation on the processing of biometric data, as well as the related opinions, guidelines and resolutions of the National Authority for Data Protection and Freedom of Information (NAIH) and the Article 29 Data Protection Working Party (WP29).

Keywords: *biometric authentication, biometric data, data protection*

A kézirat benyújtásának dátuma (Date of the submission): 2019.02.06.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.03.25.

BEVEZETÉS

Napjaink egyre növekvő mértékű digitalizációja következtében a természetes személyek és a gazdaság különböző szereplőinek egyre több adata digitális formában kerül létrehozásra, tárolásra. Részben emiatt is folyamatosan nő az igény a nagy megbízhatóságú, gyors és a felhasználók számára kényelmes, egyszerű személyazonosítási módszerek iránt.

Az egyre gyorsuló ütemű technológiai fejlődés, valamint a szenzorok olcsó tömegcikké válásának hatására a biometrikus azonosításra szolgáló eszközök ma már széles körben elérhetővé váltak, így sok esetben alternatívát jelentenek, vagy kombinált használatot tesznek lehetővé a tudás, illetve tulajdon alapú személyazonosítási módszerekkel.

A termékfejlesztési ciklusok a piaci verseny hatására időben folyamatosan rövidülnek, ami kihatással van a biometrikus technológiák tömeges terjedésére és alkalmazására is. Mind a társadalomnak, mind a jogalkotónak időre van azonban szüksége ahhoz, hogy felmérje a technológiai fejlődés jogi és társadalmi hatásait és ennek alapján meghozatalra kerüljenek a szükséges intézkedések, kialakításra kerüljön a megfelelő jogi környezet. A jogszabályi környezettel kapcsolatban egyrészt alapvető elvárás, hogy ne korlátozza szükségtelenül az innovációt és a fejlesztést, másrészt viszont tegye átláthatóvá a biometrikus adatok kezelését és nyújtson megfelelő garanciákat az érintettek jogai védelmének érdekében.

A BIOMETRIA ÉS A BIOMETRIKUS AZONOSÍTÁS MŰKÖDÉSI ELVE

A biometria kifejezés görög eredetű összetett szó, mely az életet jelentő „bio” és a mérést jelentő „metria” szavakból áll. [1] A biometria egy fizikai vagy biológiai jellemző vagy attribútum amely mérhető. [2] A biometria tehát egy ember mérhető testi, illetve viselkedésbeli jellemvonása, amely alkalmas arra, hogy mérésével az ember azonosságát ellenőrizni lehessen. [3]

A biometrikus azonosítás működési elve

A biometrikus azonosítás menete két szakaszra osztható. Az első szakasz magában foglal minden olyan folyamatot, amely a biometrikus adat kinyeréséhez, annak biometrikus sablonná történő átalakításához és digitalizálásához, az érintettel történő összekapcsolásához, valamint tárolásához szükséges. Ezt regisztrációs szakasznak nevezik, amely jellemzően az első alkalom, amikor az érintett kapcsolatba kerül a biometrikus rendszerrel. Mind a regisztráció során kinyert biometrikus adatok mennyiségének, mind a minőségének elegendőnek kell lennie ahhoz, hogy lehetővé tegye az érintett személy megbízható azonosítását. A második szakasz az azonosítás, amely során a kinyert biometrikus adatok a digitalizálást követően összehasonlításra kerülnek a korábban kinyert és a rendszerben eltárolt sablonnal.

A biometrikus adatok kezelésének jogi szabályozása

Az Európai Parlament és a Tanács 2016. április 27. napján elfogadta 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) (a továbbiakban: GDPR) szóló rendeletet, amely 2018. május 25. napjával hatályon kívül helyezte a korábbi, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelvet. Az uniós jogforrási hierarchia alapján a rendelet olyan kötelező jogi aktus, amely általános hatállyal bír, teljes egészében kötelező, közvetlenül alkalmazandó és a címzetteknek maradéktalanul be kell tartaniuk anélkül, hogy a tagállamoknak át kellene azt ültetniük saját nemzeti jogukba. A GDPR tehát az Európai Unió egész területén teljes egészében alkalmazandó, így felváltva a korábbi tagállamonként tagolt irányelvi szabályozási rendszert,

egységes adatvédelmi rezsimet létrehozva az Európai Unió és az Európai Gazdasági Térség területén. Ennek következtében a korábbi tagállami szintű adatvédelmi jogszabályok minden tagállamban jelentősen módosításra kerültek, hatályukat csak a GDPR által eltérést megengedő, vagy nem szabályozott kérdéskörökre szorítva.

A GDPR alapján biometrikus adatnak minősül egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat. [7, 4. cikk 14.] Az arcot ábrázoló fényképek kezelését nem szükséges azonban szisztematikusan különleges adatkezelésnek tekinteni, mivel azokra csak azokban az esetekben vonatkozik a biometrikus adatok fogalommeghatározása, amikor a természetes személy egyedi azonosítását vagy hitelesítését lehetővé tevő speciális eszközzel kezelik őket. Ez alapján egy egyszerű, természetes személyt ábrázoló fénykép még nem minősül biometrikus adatkezelésnek, azonban ha a fényképeket egy arcfelismerő algoritmus kezeli, úgy az már biometrikus adatkezelésnek számít.

A biometrikus adatok kezelésére vonatkozó előírások ismertetése előtt fontos tisztázni azt, hogy a jogszabály definíciója szerint mi számít adatkezelésnek. A meghatározás szerint adatkezelésnek minősül a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés. Az exemplifikatív felsorolás hosszasan sorolja az adatkezelésnek minősített leggyakoribb műveleteket, azonban a definíció első feléből egyértelmű, hogy a személyes adatokon végzett bármely olyan művelet adatkezelésnek minősül, amely kiterjed a személyes adatok kezelésére.

A 40. Prembulumbekezdés alapján a személyes adatok kezelése csak megfelelő jogalap fennállása alapján lehetséges. Az adatkezelés csak megfelelő jogalap fennállása esetén jogszerű, így mindenképpen szükséges, hogy az adatkezelő az adatkezelés jogalapjaként legalább egy jogalapot megnevezzen a jogalapok 6. cikk (1) bekezdésben található zárt és véges felsorolásából. [4, 95. o.] Egy adatkezelés azonban több jogalap alapján is történhet. Ebben az esetben, amennyiben az elsődleges jogalap megszűnik, úgy a másodlagosan megjelölt jogalap lép a helyébe.

A GDPR kiindulópontja az, hogy a személyes adatok különleges kategóriáinak és az ebbe a körbe tartozó biometrikus adatoknak a kezelése tilos, tekintettel arra, az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az érintettek jogaira nézve a kezelésük körülményei jelentős kockázatot hordozhatnak. [7, 51. Preambulumbekezdés] Ezért a biometrikus adatok kezelése csak abban az esetben jogszerű, amennyiben a 6. cikk szerinti jogalaptól 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. [4, 141. o.] A GDPR lehetővé teszi a tagállamok részére, hogy további feltételeket – köztük korlátozásokat – tartsanak hatályban, illetve vezessenek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.

A 29. cikk szerinti Adatvédelmi Munkacsoport (a továbbiakban: Munkacsoport) – melynek helyébe 2018. május 25. napját követően az Európai Adatvédelmi Testület lépett – a biometrikus adatok kezelésének követelményeit részletesen elemezte a biometrikus technológiák terén történt fejleményekről szóló véleményében [9]. A Munkacsoport rögzítette, hogy a biometrikus adatok csak abban az esetben kezelhetők, ha rendelkezésre áll megfelelő

jogalap és a gyűjtésük, illetve további kezelésük célja szempontjából a kezelés megfelelő, releváns és nem túlzott mértékű.

A biometrikus adatok kezelésének alapelvei

Fentebb idézett véleményében a Munkacsoport megjelölte a célhoz kötöttség, az arányosság, a pontosság, az adatminimalizálás és a korlátozott megőrzés elvét, mint a biometrikus adatok kezelésének alapvető elveit. Ezen elvek megfeleltethetőek a GDPR személyes adatok kezelésére vonatkozó alapelveinek.

Arányosság

A személyes adatok kezelése során elvárás, hogy a kezelt személyes adatok köre arányban álljon az elérendő céllal. Az arányosság elve négy szempont mérlegelését teszi szükségessé az adatkezelés arányosságának megállapítása céljából. Először is mérlegelni szükséges, hogy a biometrikus adatok kezelésével megvalósuló adatkezelés valóban szükséges-e a meghatározott cél eléréshez, vagy annak csak egy kényelmes és költséghatékony módja. A második szempont a rendszer hatékonyságának vizsgálata, összehasonlítva más, kisebb mértékű adatkezeléssel járó módszerhez képest. Harmadik szempontként szükséges vizsgálni azt, hogy arányosak-e a biometrikus adatokat kezelő rendszer kiépítésével járó előnyök az érintettek jogainak korlátozásához viszonyítva. Az arányosság megállapítása érdekében negyedik szempontként vizsgálandó, hogy a biometrikus adatok kezelésével járó rendszerhez képest a magánéletbe kisebb mértékben beavatkozó rendszerek alkalmasak lehetnek-e elérni a megvalósítandó célt?

A Munkacsoport példaként egy egészség- és fitneszklubot hoz fel, ahol ujjnyomatok gyűjtésén alapuló központosított biometrikus rendszert vezetnek be, amely az összes vendég és alkalmazott ujjlenyomatát tárolná. Egy ilyen beléptető és azonosító rendszer kiépítése aránytalannak minősül, tekintettel arra, hogy az elérendő cél (a belépés ellenőrzése és a bérletek kezelése) más, biometrikus adatok feldolgozását nem igénylő módszerekkel is megvalósítható, mint amilyen például egy RFID cimke. [9] A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) a munkahelyi adatkezelések alapvető követelményeiről szóló tájékoztatójában a Munkacsoport állásfoglalását összegezve rögzíti, hogy az arányosság vizsgálata során az adatkezelő minden esetben köteles ellenőrizni, hogy egyes alternatív intézkedések lehetnének-e a kitűzött célra tekintettel ugyanolyan hatékonyak, de kisebb beavatkozással járók. [5, 35. o.] Amennyiben rendelkezésre állnak ilyen alternatívák, úgy az adatkezelő az arányosság elvének megfelelően köteles ezeket az alternatívákat választani.

Jogszerűség, tisztességes eljárás és átláthatóság elve

Az alapelvek közül az első, amely általános jelleggel rögzíti a jogszabályok tiszteletben tartásának követelményét és egyben feltételezi a megfelelő jogalap meglétét. [7, 5. cikk] Amint az fentebb már említésre került, a biometrikus adatok kezelése esetén az adatkezelőnek rendelkeznie kell nem csak a megfelelő, törvényes jogalappal, de meg kell felelnie valamely 9. cikk szerinti speciális feltételnek is. A törvényes jogalapon meglétén túlmenően az adatkezelésnek az egész folyamat alatt meg kell felelnie a tisztességesség és átláthatóság követelményének is. Az adatkezelés tisztességessége garantálja az emberi méltóság védelmét, míg az átláthatóság elősegíti az érintettek tájékoztatását és jogainak gyakorlását azáltal, hogy az adatkezelés folyamata dokumentált, a külvilág számára is transzparens, megismerhető, melyet az érintett közérthető, világosan megfogalmazott és könnyen hozzáférhető tájékoztatásból ismerhet meg.

Célhoz kötöttség

Az egyik legfontosabb alapelv, amely szorosan kapcsolódik a fentebb felsorolt jogszerűség, tisztességes eljárás és átláthatóság elvéhez. A célhoz kötöttség elve megkívánja, hogy

személyes adatok – beleértve a biometrikus adatokat is – gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. [7] A célhoz kötöttség elve tehát megköveteli, hogy az adatkezelő még az adatkezelés megkezdése előtt meghatározza az elérendő célokat és az annak érdekében szükséges személyes adatok körét. Csak így dönthető el, hogy mely személyes adatok szükségesek az adott cél eléréséhez. A célhoz kötött adatkezelés azért is kiemelt jelentőségű, mert az Alkotmánybíróság máig ható elvi éllel rögzítette határozatában, hogy „a meghatározott cél nélküli, előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés- és tárolás alkotmányellenes", rögzítve ezzel a készletező adatgyűjtés máig tartó tilalmát. [13] Korunk robbanásszerű digitális fejlődését megelőzve, a rendszerváltozás előtti diktatórikus gyakorlatokra tekintettel mondta ki az Alkotmánybíróság, hogy a korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása alkotmányellenes, mert az az érintettett az adatkezelővel szemben kiszolgáltatottá teszi, egyenlőtlen helyzetet teremtve ezzel. Napjainkban azonban már nem csak az államok, mint orwelli „nagytestvérek" gyűjtenek adatokat az érintettekről, hanem a gazdasági élet legtöbb szereplője is törekszik valamilyen profil kialakítására az érintettekkel kapcsolatban összegyűjtött adatok alapján. A célhoz kötöttség elve alapján a biometrikus adatok használatának előfeltétele az adatkezelés céljának egyértelmű meghatározása, figyelembe véve az egyének alapvető jogainak és szabadságának védelmét érintő kockázatokat is.

Pontosság

Egy természetes személy adatai az idő előrehaladtával változhatnak. Vannak azonban olyan egyedi azonosításra alkalmas személyes adatok, amelyeket nem érint az idő múlása. Ezen adatok körébe tartozik a biometrikus adatok nagy része is[1], melyek éppen ezért alkalmasak a természetes személyek nagy pontosságú azonosítására. Garanciális jelentősége van tehát a pontosság elvének a biometrikus adatok kezelése során, amely egyben kötelezettséget is jelent a biometrikus adatok felvétele és a sablonképzés során a pontos adatrögzítésre, valamint a sablonok precíz tárolására. A pontatlan adatbevitelből eredő hátrányok következményei jelentősek lehetnek, ezért alapvető követelmény, hogy a pontatlanul rögzített személyes adatok a tudomásszerzést követően a lehető leghamarabb helyesbítésre vagy törlésre kerülhessenek. [GDPR 5. cikk (1) bekezdés d) pont].

Adattakarékoság

A biometrikus adatok kezelésével kapcsolatban a Munkacsoport által megfogalmazott adatminimalizálás, azaz a szükségesség kritériuma, adatakatékosság elveként került megfogalmazásra a GDPR-ban. Az adatakarékosság elve alapján a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek és a szükségesre kell korlátozódniuk. Ez az elv, szoros összefüggésben a célhozkötöttség elvével, meghatározza az adatkezelés terjedelmi és időbeli korlátját, amely alapján csak annyi és olyan adat kezelhető, amely szükséges és egyben elégséges az adatkezelés céljának eléréséhez. [4, 101. o.] A biometrikus azonosító rendszerek esetében ez a gyakorlatban azt jelenti, hogy az adott rendszerrel megvalósítani kívánt biztonsági szint eléréséhez szükséges legkevesebb adatot kell felhasználni a biometrikus sablon elkészítéséhez.

[1] Például az írisz, amely a retinával ellentétben nem változik sem a betegségek, sem az öregedés során.

Korlátozott tárolhatóság

A személyes adatok és ezáltal a biometrikus adatok tárolásának is olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. [7 5. cikk e) pont] Az adatkezelőnek tehát megőrzési időszakot kell meghatároznia a biometrikus adatokra vonatkozóan, amely nem lehet hosszabb, mint az adatkezelés céljainak eléréséhez szükséges idő. Az adatkezelőnek biztosítania kell, hogy a kezelt adatokat vagy az adatokból származtatott további adatokat, profilokat véglegesen töröljék, vagy helyreállíthatatlanul anonimizálják ennek az indokolt időszaknak az eltelte után.

Integritás és bizalmas jelleg

Új elvként került nevesítésre a személyes adatok kezelésére vonatkozó alapelvek között az integritás és bizalmas jelleg elve, amely korábban, mint az adatbiztonsággal kapcsolatban megfogalmazott elvárás volt jelen az irányelvi szabályozásban és azzal párhuzamosan a hazai szabályozásban is. Az adatkezelés során a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. [7 5. cikk f) pont] Az elv alapján a rendelkezésre álló magasabb szintű védelmet biztosító megoldást kell választani, tekintettel a technika fejlettségének szintjére is. Az adatkezelés biztonságára vonatkozó konkrét követelményeket a GDPR 32. cikke tartalmazza. „Az adatok integritása jelenti az adatminőség garatnálását, az adatok pontos, teljes rendelkezésre bocsátásának lehetőségét a hozzáférésre jogosultaknak, és az adatok megóvását valamennyi külső, nem várt hatástól, a szándékos beavatkozástól a hanyag emberi magatartásokig.” [4, 107. o.]

Az adatok biztonságának kockázatokkal arányos, megfelelő szintű biztosítása alapvető követelmény az adatkezelővel szemben, hiszen az adatok elvesztése, megsemmisülése, jogosulatlan kezelése vagy az azokhoz történő hozzáférés fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintettek számára. A biometrikus adatokat tároló adatbázisok, mint például a DNS-mintákat tároló orvosi vagy kutatási célú adatbázisok, eddig is kiemelt célpontjait képezték a támadásoknak Az Egyesült Királyságban 2013-ban indult el a „100,000 Genom Projekt”, amelynek célja egy DNS adatbázis felépítése a szigetországban, valamint pontos diagnózis felállítása és lehetséges gyógymódok felkutatása a projektben résztvevő személyek DNS-mintáinak elemézse által. A projekt során több, mint 85.000 résztvevő DNS-mintáját tárolták a kutatók. A sorozatos támadások következtében a kutatás alapjául szolgáló biometrikus adatokat át kellett helyezni az Egyesült Királyság védelmi minisztériumának egyik fokozottan védett létesítményében található szervereire. [15]

A biometrikus adatok bűnmegelőzési és bűnüldözési felhasználása

A biometrikus adatok egyik legrégebbi felhasználási területének a bűnüldözés számít, elég csak a daktiloszkópiára és a több, mint száz éves múltra visszatekintő ujjnyomatokra épülő magyar bűnügyi nyilvántartásra gondolni. A technikai fejlődés azonban ezen a területen is megvalósíthatóvá tett korábban csak a tudományos-fantasztikus irodalomban és filmekben felvázolt lehetőséget.

Földesi Krisztina 2014-ben vizsgálta a biometrikus technikákat érintő társadalmi attitűd, averzió mértékét a Fejér Megyei Rendőrfőkapitányság hivatásos állományának, valamint az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar hallgatóinak és oktatóinak körében. [6] A vizsgálat a biometrikus technikák elfogadottságán túlmenően kiterjedt az esetleges elutasítás okaira is. A kérdőíves kutatásban a résztvevőknek többek között arra a kérdésre kellett válaszolniuk, hogy támogatnák-e az elektronikusan rögzített ujjlenyomat nyilvántartás kiterjesztését minden emberre, hogy születéskor minden gyermek íriszmintája rögzítésre és tárolásra kerüljön-e egy központi adatbázisban a rendőrség által, hogy létrehozásra kerüljön-e egy arc azonosító-körözési adatbázis, továbbá, hogy bizonyos meghatározott

bűncselekmények esetén az ujjlenyomaton túlmenően el elítéltek egyéb biometrikus adatadatai (DNS, ujjlenyomat stb.) rögzítésre kerüljenek-e.

A kutatás megállapításai és a társadalom véleményének vizsgálata napjainkban különösen aktuális, ugyanis Kínában 2020-ra tervezik a társadalmi kreditrendszer bevezetését [10], amely segítségével a kínai állam az állampolgárok elektronikus profiljához társított pontszámon keresztül tud majd közvetlen hatást gyakorolni az emberek hétköznapjaira. Kínában már jelenleg is hatalmas méretű, megközelítőleg 200 millió kamerából álló kamerás megfigyelőrendszer működik. [11] Ez elől a világon egyedülálló méretű megfigyelőrendszer elől nem maradhat rejtve szinte senki, nyilvános helyeken elbújni nem lehet, ugyanis a nagy pontosságú arcfelismerő rendszer mellett jelenleg már folynak a helyi kísérletek járásfigyelő alkalmazások használatára is, amelyek a járás és testalkat alapján képesek megkülönböztetni az a megfigyelt személyeket. [16] A kérdés tehát már régen nem a megvalósíthatóság, hanem a létrehozásra irányuló akart és az ezt lehetővé tévő jogi szabályozás.

A kutatási eredmények alapján mindkét vizsgált csoport nagyrésze támogatta a bűncselekményben érintett személyekre vonatkozó biometrikus adatrögzítés kiterjesztését, az elektronikusan rögzített ujjlenyomat nyilvántartás kiterjesztését inkább a rendőrök támogatták, míg az egyetemisták több mint fele elutasította azt. A születéskori íriszminta rögzítést és tárolást mindkét csoport markánsan elutasította. A társadalom nagy része feltehetőleg szintén elutasítana egy születéskori íriszmintavétel gondolatát.

A kutatás alapján a bűnmegelőzés és bűnüldözés hatékonyságának javítása érdekében konkrét javaslat is megfogalmazásra került. Egy a rendőrség által kezelt központi adatbázis formájában, amely valamennyi magyar állampolgár meghatározott biometrikus adatait és azonosító kódját tartalmazá. A rendszer kialakításának első lépése lenne a már működő adatbázisok kompatibilitásának megteremtése, bűnüldözési célú felhasználása. [6, 138. o.]

Magyarországon jelenleg is tartalmaz a bűnügyi nyilvántartás biometrikus adatokat. A törvény részletesen meghatározza a nyilvántarott biometrikus adatok körét, valamint felhasználásuk célját, megőrzésük idejét és az érintetteket megillető garanciális szabályokat. [12] A DNS-nyilvántartás célja a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzített anyagmaradvány alapján a bűncselekmény elkövetésével összefüggésbe nem hozható, a bűncselekményt elkövető, valamint a rendkívüli haláleset miatt folyó közigazgatási hatósági eljárásban az ismeretlen személyazonosságú elhunyt személy azonosítása.

Egy ilyen központi adatbázis létrehozásának legfőbb indoka a személyes adatok védelméhez fűződő alapvető jog, amely minden természetes személyt megillet. A személyes adatok védelméhez fűződő alapvető jog először az Emberi Jogok Európai Egyezményének 8. cikkében került rögzítésre, amely rögzíti, hogy mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák. [14] Ebből a minden természetes személyt megillető alapvető jogból került levezetésre a személyes adatok védelméhez való jog. Az Egyezmény alapján az Emberi Jogok Európai Bírósága számos esetben vizsgálta a személyes adatok védelmének jogát és e jog korlátozhatóságának határait. Az Egyezmény maga fogalmazza meg ezt a korlátot, amikor kimondja, hogy a magánélet tiszteletben tartásához való jog gyakorlásába hatóság "csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az országgazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.". Ezek a korlátozások azonban mindenképpen arányosak és alkotmányosan indokoltak kellenek, hogy legyenek. Éppen ezért a jelenleg létező és korlátozott célú, biometrikus adatokat tároló nyilvántartások összekötése és a társadalom minden tagjára történő kibővítése nem reális forgatókönyv. Egy akár íriszmintán, akár DNS mintán alapuló adatbázis létrehozásához szükséges lenne a mintavétel Magyarország teljes lakosságától. Egy ilyen adatbázis kiépítése

ugyan technikailag kivitelezhető lenne, azonban a jelen jogszabályi környezetben egészen biztosan nemzetközi szerződésekbe ütközne és alkotmányellenesnek minősülne, mivel az ilyen adatbázis által alkalmazott általános és egységes biometrikus azonosító kód sértené a célhoz kötött adatkezelés és a készletező adatgyűjtés tilalmát. A NAIH javaslatában [17] kifejezetten javasolta „az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) általános érvénnyel előírni, hogy Magyarországon nem hozható létre a teljes népességre kiterjedő biometrikus referencia adatbázis." Ugyan ez a tilalom szövegszerűen nem került bele az Infotv-be, de a magánélethez, valamint a személyes adatok védelméhez fűződő jog olyan alkotmányos alapérték, amelyet Magyarország Alaptörvénye, valamint számos nemzetközi egyezmény [14] és ágazati jogszabály is védelemben részesít. A felmérések alapján a társadalom körében azonban nem mutatkozik olyan elsöprő erejű igény az ilyen biometrikus adatbázisok létrehozására, amely alapjául szolgálhatna a megvalósításhoz szükséges jogszabályok mélyreható reformjának.

KÖVETKEZTETÉSEK

Jelen cikkben törekedtem arra, hogy az adatkezelés fogalmának ismertetésétől kezdődően bemutassam a biometrikus adatok kezelésére vonatkozó szabályokat és azokat az elveket, amelyeket már a biometrikus adatok kezelésének tervezése során szem előtt kell tartania minden adatkezelőnek. Az alapelvek és a konkrét szabályok azonban nem csak az adatkezelési folyamatokra, de az adatkezelést megvalósító konkrét eszközök tervezésére és kivitelezésére is hatással vannak, ezáltal közvetlenül befolyásolva az innovációt és technikai fejlődést. Amennyiben az adatkezelők számára az adatkezelési cél megvalósítása érdekében rendelkezésre áll biztonságosabb, az érintettek jogaira kevésbé kockázatos megoldás, úgy az adatvédelem alapelveinek szellemében azt kell választaniuk.

Az Európai Unió adatvédelmi reformcsomagjával markáns választ adott a digitalizáció jelentette kihívásokra és a személyes adatokra leselkedő kockázatokra. Ez a válasz jelentősen eltér a fentebb ismeretett kínai, vagy a világ más részein kialakuló egyéb rendszerektől. A biometrikus adatok előnye és hátránya is abból a tényből fakad, hogy megmásíthatatlanul az érintett személyéhez köthetők, ezért egy tudás, vagy birtoklás alapú azonosításhoz képest a biometrikus adatok bizalmasságának, sértetlenségének, hitelességének, funkcionalitásának vagy rendelkezésre állásának elvesztése olyan súlyos helyzetet teremt, amely során az esetleges hátrányos következmények enyhítése már nehezen megvalósítható. Éppen ezért, valamint az érintettek kiszolgáltatottsága, magánéletük védelme érdekében helyénvaló és indokolt a biometrikus adatok kezelésére vonatkozó szigorúbb szabályozás. Fontos lenne, hogy a társadalom megfelelő mennyiségű és minőségű információhoz juthasson a biometrikus adatok felhasználásával, alkalmazásukból számrazó előnyökkel és lehetséges kockázatokkal kapcsolatban.

FELHASZNÁLT IRODALOM

[1] KOVÁCS T. - MILÁK I. - OTTI Cs.: A biztonságtudomány biometriai aspektusai http://www.pecshor.hu/periodika/XIII/kovacsti.pdf, (letöltve: 2018.11.01.)

[2] Biometrics at the Frontiers: Assessing the Impact on Society For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), 2005. EUR 21585 EN 35. o.

[3] BALLA J.: Biometrikus adatok a személyazonosításban http://www.pecshor.hu/periodika/XIV/ballaj.pdf, letöltés: 2018. november 01.

[4] PÉTERFALVI A., RÉVÉSZ B., BUZÁS P.: Magyarázat a GDPR-ról, Budapest, 2018

[5] A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről; https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf (letöltve: 2018.12.10.)

[6] FÖLDESI K., A biometrikus azonosítási eljárások alkalmazhatósága a rendőri munkában, Budapest, 2017, Óbudai Egyetem

[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 rendelet hatályon kívül helyezéséről*

[8] 2011. évi CXII. *törvény az információs önrendelkezési jogról és az információszabadságról*

[9] A 29. cikk szerinti adatvédelmi Munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről, WP193; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf (letöltve: 2018.12.10.)

[10] CHRISTOPHER U., Blacklists and redlists: How China's Social Credit System actually works; https://technode.com/2018/10/23/china-social-credit/ (letöltve: 2018. 12. 10.)

[11] MATTHEW C., Leave no dark corner; https://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm (letöltve 2018.12.10.)

[12] 2009. évi XLVII. *törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról*

[13] 15/1991. (IV.13.) AB határozat

[14] Emberi Jogok Európai Egyezménye

[15] RICHARD C., Brits' DNA data sent to military base after 'foreign' hack attacks – report https://www.theregister.co.uk/2018/12/06/foreign_hackers_trying_to_steal_brits_dna/ (letöltve: 2018.12.10.)

[16] DAKE K., Chinese 'gait recognition' tech IDs people by how they walk, https://apnews.com/bf75dd1c26c947b7826d270a16e2658a (letöltve: 2018.12.10.)

[17] Nemzeti Adatvédelmi és Információszabadság Hatóság, Javaslatok az Infotv. módosításával kapcsolatban, Budapest, 2014. október 17., NAIH-374-3/2013/J