A BIOMETRIKUS AZONOSÍTÁS ÉS LEHETSÉGES ADATVÉDELMI KOCKÁZATAI

Moór Vivien Rita

1. Bevezetés

Napjainkban a társadalom tagjainak legnagyobb nehézsége a fejlődő világgal való lépés megtartása és a komfortérzetük megteremtése a napról napra változó világban. A technológiai újítások nagyban befolyásolják hétköznapjainkat mind a magánéletünk, mind a munkánk során. Gondoljunk csak bele, hogy mennyi példával tudunk élni e téren. Ilyenek lehetnek például a ma már megszokottá vált okostelefonok megjelenése, az ezt felülmúló okosotthonok, okosautók bevezetése vagy éppen a munkahelyre való eljutást segítő elektromos rollerek fejlesztése.

Léteznek azonban már olyan technológiai újítások, amelyek még annyira távolinak tűnnek, hogy nem vagyunk tisztában azzal, hogy milyen nehézségekkel járhat a bevezetésük, megvalósításuk. Ilyen például a mesterséges intelligencia, a blokklánc technológia vagy éppen a biometrikus beléptető- és azonosítórendszer működtetése. De vajon milyen kihívásokat állítanak elénk a modern technológia által eszközölt újítások? Nehézségekkel jár a tudományos fejlesztések megfeleltethetősége technológiai szempontból, azonban mindemellett nem szabad szem elől tévesztenünk azt sem, hogy egy jogállamban szükséges az is, hogy jogszabályok társuljanak mellékük, amelyek keretet adnak a működésüknek.

Tanulmányom témája a technológiai újítások során felmerülő jogrendszeri nehézségek vizsgálata, központi hangsúlyt fektetve a biometrikus rendszerek bevezetésére, működésére és az adatvédelmi joggal való kapcsolatára a hétköznapi, elsősorban munkahelyi azonosítások területén. Azért ezt a kérdéskört kívánom vizsgálni, mert véleményem szerint nagy igény van a témában szereplő válaszok feltárására, illetve ez még egy nagyon gyerekcipőben járó

jogi probléma Európában. A tanulmányom alapját az Általános Adatvédelmi Rendelet[1] (továbbiakban: GDPR) adja, ami 2016. május 24-én lépett hatályba és 2018. május 25. óta alkalmazandó. A GDPR rendelkezései javarészt lefedik a fontosabb, lényegesebb eseteket, azonban vannak olyan helyzetek, ahol még a határ elmosódása vagy éppen a helyzet tisztázatlanságából fakadóan a szabályozás még nem teljeskörű.

Az adatvédelmi jog egyre jelentősebbé válásával és a GDPR bevezetésével a biometrikus beléptetőrendszerek üzemeltetése körülményesebbé vált és újabb nehézségekbe ütközött. A biometrikus azonosítás, megjelenésével kihívásokat állított a pályán dolgozó jogászok elé és ezzel egyidőben társadalmi problémává is vált, ugyanis mindannyian érintettek lettünk benne azáltal, hogy az élet minden területén részesévé váltunk. Ez megtörténhet úgy, hogy alanyai lettünk egy biometrikus azonosítórendszernek egy egyszerű használat során, mint érintett, amely esetében az egyszerű használat során már adatvédelmi kérdések vetődtek fel a rendszer megfelelőségével kapcsolatban. Az adatvédelmi közegen belül ezen túlmenően kialakult egy kérdés, amely a biometrikus adatok felhasználhatóságát tette kérdésessé. A GDPR megjelenésével vált hangsúlyossá a kérdés megválaszolása, ugyanis a legfőbb problémát a fejlett technológia, alapelvekkel összhangban való gyakorlati alkalmazása okozta.

Milyen irányelveknek kell megfelelni egy biometrikus azonosítórendszer használatakor? A jogszabályok mennyire állnak készen arra, hogy a közjó érdekében eszközölt technológiai újításokat be tudják fogadni és teret adjanak az alkalmazásuknak? Három, európai esetet vizsgálva kívánom megerősíteni azt az álláspontot, hogy jelen pillanatban a GDPR területi hatálya alá tartozó országokban, ahol már korábban próbálkoztak a biometrikus azonosítórendszer bevezetésével, mennyire elutasítók voltak gyakorlati alkalmazással szemben a hatóságok és szemléltetni fogom azt, hogy ennek oka a GDPR által eszközölt szigorú szabályok megléte volt.

A fent említett kérdéseket középpontba helyezve keresem a választ a biometrikus azonosítás és adatvédelmi jog kapcsolatára vonatkozó problémákra.

[1] 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 (általános adatvédelmi rendelet).

2. A technológia szerepe

A napról napra változó világunk mondhatni legfőbb mozgatórugója a technológia által eszközölt változások, újdonságok megjelenése. Egy-egy új találmány, alkalmazás, eszköz vagy rendszer megjelenése teljesen felborítja az addig megszokott, állandósult, változatlan életvitelünket és szükségessé teszi, hogy kissé rugaszkodjunk el a komfortzónánktól és ezáltal beépítsük az újat az életünkbe. Ezen rendszerek legtöbb esetben személyes adatok felhasználásával működnek, épp ezért fontos észrevételezni, hogy a technológiai újítások megjelenésével újabb és újabb kockázatok merülnek fel az adatok védelmével kapcsolatban. Egy igazán részletes doktori disszertációra alapozva dolgoztam fel ezt a részt, az egyénekhez legközelebb álló, leghétköznapibb példából kiindulva a tanulmányom központi témájáig, a biometrikus azonosításig.[2] Ennek a segítségével a mesterséges intelligenciát szeretném bemutatni, amely mindenki számára egyre inkább ismertté vált az elmúlt években. Vajon hol találkozhatunk a megjelenésével a hétköznapokban?

A legkézenfekvőbb példát ismertetném elsőre, amely pedig nem más, mint az *elektronikus levelezés*, amellyel mind a magánéletünk, mind a munkánk során találkozhattunk már. Kicsit távolibbnak tűnhet, de ugyanúgy a mindennapjaink részét képezik a mesterséges intelligencia alapú digitális személyi asszisztensek. A harmadik példa, amely tanulmányom központi témáját képezi nem más, mint az *azonosítórendszerek* megjelenése. Napjainkban egyre inkább rohamos fejlődést mutatnak az azonosítórendszerek és különböző megjelenési formáik.

Összegezve tehát az eddigieket, a mesterséges intelligenciáról elmondható, hogy e technológiai újítás megjelenésével rengeteg adatvédelmi kérdés vetődik fel. Az ilyen alapú rendszerek felhasználásának egyik legfőbb kockázata az, hogy rengeteg adat szükséges ahhoz, hogy ezek a rendszerek megfelelően tudjanak működni. A későbbiekre való tekintettel az adatok tárolása is elengedhetetlen, így egy több elemű adatbázist kiépítve a rendszer nagyon sok személyes adatot őriz meg több hónapon vagy akár éveken át. Az említett adatok megadása elengedhetetlen feltétele a rendszer működésének, így a felhasználók a használattal beleegyeznek abba, hogy adataikat rendelkezésre bocsájtják és a fent feltett kérdésekbe mind beleegyeznek. Ezek alapján megállapítható, hogy

[2] Stefán Ibolya: A mesterséges intelligencia adatvédelmi vonatkozásai. In: Barzó Tímea – Csák Csilla – Dmitro Bielov – Yaroslav Lazur – Sibilla Buletsa (szerk.): *Modern Researches: Progress of the legislation of Ukraine and experience of th European Union.* Part 1–2. Miskolc–Riga, Miskolci Egyetem Állam és Jogtudományi Kar – Izdevniecība Baltija Publishing, 2020. 40–41.

a mesterséges intelligencia alapú biometrikus azonosítórendszerek használata során is rengeteg adatvédelmi kérdés és biztonsági kockázat merülhet fel.

3. Az adatvédelem fejlődése

Az adatvédelmi szabályozás már a XX. században megjelent a tagállamok jogrendszerében, amely a technológiai fejlődéshez folyamatosan igazodva változott az évek során. A GDPR bevezetését megelőzte több szabályozás is, amelyeket csak említés szintjén kívánok felsorolni tanulmányomban. Ezek kronológiai sorrendben az alábbiak voltak: az Emberi Jogok Egyetemes Nyilatkozata (1948), az Emberi Jogok Európai Egyezménye (1950), a különböző nemzeti adatvédelmi törvények az 1970-es években, az Adatvédelmi Egyezmény (1981) és az adatvédelmi irányelv (1995)[3]. Az Európai Unió Hivatalos Lapjában 2016. május 4-én került kihirdetésre „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 szóló, 2016.április 27-i 2016/679/EU európai parlamenti és tanácsi rendelet (általános adatvédelmi irányelv)”[4]. Ezt követően a tagállamoknak két év állt rendelkezésükre, hogy a felkészüljenek a rendelet alkalmazására, így a GDPR 2018. május 25-én került bevezetésre és ettől a pillanattól kezdve minden EU tagállamra nézve kötelező érvényűvé vált.

A továbbiakban felmerülhet bennünk a kérdés, hogy a szabályozás egységesítését mi indokolhatta? Vajon volt-e alapja annak, hogy egy egységes jogszabály, amely az Európai Unió minden tagállamára kötelező erővel bír, szükséges volt? Gondoljunk bele abba, hogy mennyi adat áramlik a nagyvállalatokon, multinacionális cégeken keresztül az országok között akár csak a munkavállalók puszta alkalmazásával. A munkaviszony létesítését megelőzően az álláshirdetésre való jelentkezéskor, a munkaviszony fennállása alatt a különböző belső ellenőrzések során, vagy éppen társadalombiztosítási adózás céljából valósul meg az adatkezelés.[5] Egy-egy üzleti úthoz szükséges dokumentáció elkészítése vagy a belépőkártya birtoklása és az ehhez tartozó adatok begyűjtése a nemzetközi cégeknél már több országban is érintette a munkavállalók jogait. Azonban nem

[3] *Európai adatvédelmi jogi kézikönyv.* Luxemburg, Európai Unió Kiadóhivatala, 2014. 14–17.

[4] Bendik Tamás: A GDPR szabályozási környezete. In: Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.): *Magyarázat a GDPR-ról*. Budapest, Wolters Kluwer, 2018. 32.

[5] *A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető körülményeiről*, Budapest, 2016.10.28. 1.

csupán a munkaviszony fennállása alatt, hanem a megszűnése után is zajlik az adatkezelési tevékenység a volt munkavállalók nyilvántartásának céljából, nemzetközi cégek esetében különböző országokban is.[6] Ezért is volt szükséges egy egységes kodifikáció megalkotása, amely az összes EU-s tagállamra nézve kötelező erővel bírt és ugyanolyan elvárásokat támasztott a különböző országban lévő adatkezelők. Ennek következtében az érintettek az Európai Unió bármely részén ugyanazon jogaikat tudták érvényesíteni és az adatkezelők is ugyanazon kötelezettségeiknek kellett, hogy megfeleljenek a személyes adatok kezelése során.

A legtöbb jogi szakterületen található különböző alapelvekkel való találkozás megszokottá válása után nem meglepő, hogy az adatvédelmi jog területén a GDPR-hoz tartozóan is különböző alapelveket ismerhettünk meg. Ezen alapelvek betartása elengedhetetlen feltétele annak, hogy az adatkezelés működése a törvényes kereteknek megfelelő, rendeltetésszerű joggyakorlás végett valósuljon meg. Tanulmányom központi témája a biometrikus adatkezelés, amely során személyes adatkezelési tevékenység valósul meg, amelyet a meghatározott alapelveknek megfelelően köteles az adatkezelő végezni.

4. A biometrikus azonosítórendszerek gyakorlati megjelenése

A biometrikus azonosítórendszerek meghatározott adatok felhasználásával működnek, ezen adatokat pedig biometrikus adatoknak nevezzük. Elsőként nézzük tehát meg, hogy mit nevezhetünk biometrikus adatnak? A biometria szó két részből tevődik össze: a görög ’bio’ és a ’metria’ szavakból. A ’bio’ görögül az életet jelenti, míg a ’metria’ a mérést. Így a két szóból összetéve kialakult az a meghatározás, miszerint egy adott élőlény, jelen esetben az ember, valamely élettani jellemzője alapján az azonosítás segítségével mérik és állapítják meg a személyazonosságát és határozzák meg a jogosultságát.[7] A későbbiekben fogalmat a 29-es Munkacsoport tisztázta munkássága során, eszerint tehát a biometrikus adat: „biológiai jellegzetességekként, viselkedési vonatkozásokként, pszichológiai sajátosságokként, életvitelként vagy olyan ismétlődő tevékenységekként, amelyek során e jellegzetességek és/vagy

6 Eszteri Dániel: A GDPR tárgya. In: Péterfalvi–Révész–Buzás i. m. 49–54.

7 Kovács Tibor – Milák István –Ott Csaba: A biztonságtudomány biometriai aspektusai. Pécsi Határőr Tudományos Közlemény, XIII. kötet, 2012. 485.

tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi”[8]. A biometrikus adat forrását két csoportra bonthatjuk, beszélhetünk az érintett fizikai, fiziológiai jellemzőit feldolgozó, például az ujjnyomat ellenőrző, arcfelismerő, hangfelismerő, DNS-felismerő, rendszerekről. A másik csoportban pedig az érintett viselkedését vizsgáló technikákat sorolhatjuk, ahova pedig a járásmód elemzése vagy az érzelmi állapot hang alapú felismerése tartozik.[9]

A biometrikus adatok előnye az, hogy több olyan jellemző tulajdonsággal rendelkeznek, amelynek köszönhetően más-más területen kerülhetnek felhasználásra.[10] Segítségünkre lehetnek az érintettek azonosításában, ahogy a biometrikus azonosítórendszereknél is teszik, az ellenőrzésükben, a profilalkotásban, továbbá abban is, hogy megtaláljuk ezek segítségével az érintett személyt abban az esetben, ha éppen úgy érezzük, hogy nyoma veszett.[11] Ha a fent említett mondatra gondolunk vissza úgy érezhetjük, hogy az érintett megfigyelés áldozatául esik a biometrikus azonosítórendszerek használata révén. Ez a feltételezés megalapozott lehet azért, mert az egyén magánszférájába úgymond bekerülünk azáltal, hogy ilyen mértékben betekintést nyerhetünk az életébe és annak minden egyes mozzanatába, vagy éppen azért, mert szinte bármikor megtudhatjuk a tartózkodásának pontos helyét egy DNS-minta alapján. Ezek alapján megállapítható, hogy az érintett magánélete és az adatvédelmi jog szoros kapcsolatba állnak egymással. Ebben az esetben szintén kétségek merülhetnek fel az érintett részéről, ezért fontos, hogy a technológiai újítások ellenére is biztosítva legyen a személyes adatok védelme az adatalanyok számára.[12] Mivel a biometrikus adat örök érvényű, nem másítható meg vagy módosítható az évek alatt, ezért különösen érzékeny adatnak minősül. A biometrikus adat továbbá személyhez kötött, ezért megállapítható, hogy két egy petéjű iker sem rendelkezik egyforma, azonos biometrikus adattal, például DNS-sel vagy ujj-

[8] A 29-es Munkacsoport 4/2007. számú véleménye a személyes adat fogalmáról, 2007. június 10. https://bit.ly/39O4oOk

[9] A 29-es Munkacsoport 3/2012. számú véleménye a biometrikus technológiák terén történt fejleményekről, 2012. április 27. https://bit.ly/3gi96or

[10] Milan Petkovic – Willem Jonker: *Security, Privacy, and Trust in Modern Data Management*, Berlin, Springer-Verlag, 2007. 9–10.

[11] Tóth András: *Technológiai jog – Új globális technológiák jogi kihívásai,* Budapest, Patrocinium, 2016. 62–63.

[12] Tóth i. m. 63.

nyomattal[13]. Erre való tekintettel még fontosabb, hogy ezen adatok védelmére és elhatárolására fokozottabb figyelmet fordítson az adatkezelő a technikai fejlődés mindenkori állása szerint, így az érintettek magánszférája továbbra is kifogásolhatatlan védelemben részesül az adatkezelés és a tárolás ideje alatt.

A fent említett okok eredményezték azt, hogy a GDPR is a biometrikus adatot a különleges adatkategóriák közé tartozóként sorolja fel.[14] Erre vonatkozólag még szigorúbb szabályok társulnak hozzá és még fokozottabb védelem jár az érintetteknek abban az esetben, ha biometrikus adatkezelés alanyaivá válnak.[15]

4.1. A biometrikus azonosítás

A biometrikus azonosítás alapja a korábban már ismertetett biometrikus adat, hiszen ez az adat szolgál az egyén adatbázisba történő regisztrálására. A biometrikus adat meglétével önmagában azonban nem valósul meg a biometrikus azonosítás, ehhez szükséges még egy olyan fejlettséggel rendelkező rendszer megléte, amely képes feldolgozni a kapott információt, azaz felismerni az adat alapján az érintettet. A gép, amely azonosítja az adatot egy meghatározott adatbázisból dolgozik, amelyben már az adatokat rögzítették az azonosítást megelőzően. A folyamat során az érintett valamely biometrikus tulajdonságát hasonlítja össze egy, a már az adatbázisban szereplő adattal és az egyirányú titkosításnak köszönhetően biztosítja azt, hogy az adatok hozzáférhetősége korlátozott legyen. Ennek értelmében az érintettek adatai nagyobb biztonságban vannak, mivel a biometrikus adatot nem lehet visszafejteni.[16]

A biometrikus azonosítás egy olyan folyamat, amely három fázisból tevődik össze, ezek: „a regisztráció (adatfelvétel), a tárolás (adatbázis) és az azonosítás (összehasonlítás)”[17]. Az ilyen jellegű azonosítórendszerek esetén több feltétel, azonos időben történő teljesülése szükséges ahhoz, hogy a rendszer képes legyen azonosítani az adatot. Tapasztalatok alapján azonban előfordult már több olyan helyzet, amikor az érintett által már többször használt biometrikus

---

13 Ruggero Donida Labati – Vincenzo Piuri – Fabio Scotti: *Tocuhless Fingerprint Biometrics.* Boca Raton, Taylor & Francis Group, 2015. 39–42.

14 Sanjay Sharma: *Data Privacy and GDPR Handbook*. New Yersey, John Wiley & Sons, 2020. 74.

15 Klein Tamás– Tóth András (szerk.): *Technológiai jog - Robotjog – Cyberjog*, Budapest, Wolters Kluwer, 2018. https://mersz.hu/dokumentum/YOV1766__26

16 Working document of the Article 29 Working Party on biometrics, 1 August 2003.

17 Klein–Tóth i. m. 28.

adatot a rendszer valamilyen okból kifolyólag nem ismerte fel.[18] Hiába a pontos azonosítás, vannak olyan külső ráhatások, amelyek gyorsan befolyásolják az egyén a bőrének puhaságát, vagy éppen vastagságát, amely a biometrikus azonosítórendszerek működésében problémákat eredményez. A legnépszerűbb megjelenési formája az ujjnyomat alapú azonosítás, amelyet már a 19. században is alkalmaztak.[19] A későbbiekben már az Egyesült Államokba való belépéskor a reptereken is ujjnyomat mintavétel segítségével azonosították a beérkező látogatókat, amely feltétele volt az Államokba való belépéshez.[20] Létezik azonban már ennél elterjedtebb módja az ujjnyomat alapú azonosítórendszereknek, amely pedig az okostelefonok feloldásánál jelent meg.[21]

Az ujjnyomattal történő azonosítás azért is annyira elterjedt, mert megkönnyíti, meggyorsítja a folyamatokat azáltal, hogy pár másodperc alatt képes beazonosítani az értintett személyt. Nagyon pontos az ujjnyomat, ugyanis a többi biometrikus adattal összehasonlítva megállapítható, hogy a hiba esélye alacsony, amely azt jelenti, hogy a FAR mutatója[22] alapján 1.000.000 helyes azonosításra jut 1 téves.[23] Munkáltatói oldalról költséghatékonyság szempontjából is különböző előnyökkel jár az ujjnyomatos beléptetés, ugyanis a plasztikkártyák megvásárlásától, a beprogramozáshoz szükséges munkavállaló alkalmazásától, illetve az ehhez tartozó adminisztratív munkát végző munkavállaló foglalkoztatásától is megkíméli magát. A mai rohanó, egyre változó világban, ahol a technológia és a robotizáció fejlődése egyre előrébb tart, már egy munkahelyen is indokolt lenne azon igény beteljesülése, hogy a gépek által elvégezhető feladatokat ne egy vagy több munkavállaló végezze el, hanem ha van rá mód, akkor automatizálják ezeket.

Az ujjnyomat hátránya azonban az, hogy rengeteg helyen fellelhető, tehát akárhova nyúlunk, ott marad az ujjnyomatunk egésze vagy egy része. Így, a hamisítás egy 'elhagyott' ujjnyomat megszerzésével könnyen megvalósulhat más személyazonosságának visszaélésével vagy esetleg gyanúba keverhetnek

---

18 Klein–Tóth i. m. 27.

19 Szigetvári Oszkár: A magyar bűnügyi nyilvántartás kezdete. In: Parádi József (szerk.): *Ünnepi parergák Boda József 65. születésnapja tiszteletére*. Budapest, Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság, 2018. 176–177.)

20 DHS's Automated Biometric Identification System IDENT – the heart of bimetric visitor identification in the USA. https://bit.ly/36MxP0Z)

21 Sinji Mitra – Mikhail Gofman: *Biometrics in a Data Driven World, Trends, Technologies and Challenges*. Boca Raton, Taylor & Francis Group, 2017. 205–206.

22 FAR = téves elfogadási hányad

23 *Biometrikus azonosítás,* https://bit.ly/39P1GrA

más személyt a valódi elkövetők.[24] Nem csupán a személyiség lopás valósulhat meg ezáltal, hanem súlyos adatbiztonsági kérdések is felmerülhetnek az esetleges kiszivárgások következtében.[25] Ezekre való tekintettel kérdéses az, hogy milyen jogorvoslati lehetőségekkel élhetnek az érintettek ilyen esetekben?

A biometrikus azonosítás egyéb megjelenési formái, tehát például a hang, tenyér- és csuklónyomat, talpnyomat, ujjerezet, tenyérerezet, testhőkép, kézgeometria, írisz, retina, arc és DNS azonosítás is ugyanazon elvek alapján működik, mint a korábban általam részletezett ujjnyomat alapú azonosítás.[26]

5. Az eddig felmerült jogi problémák Európából

A biometrikus azonosítás egyre több helyen történő gyakorlati megjelenésének köszönhetően, a hatóság már több ügyében is foglalkozott mind hazai, mind nemzetközi szinten a biometrikus adatkezelés kérdéskörével.

5.1. A holland hatóság joggyakorlata

Kronológiai sorrendben haladva, elsőként a holland adatvédelmi hatóság (továbbiakban: DPA) által 2020. április 30-án nyilvánosságra hozott határozatot vizsgálom, amelyben 725.000 Euró bírságot szabott ki a munkáltatóra. Az ügy központi témája a munkavállalók ujjnyomatának munkáltatói oldalról történő jogellenes kezelése volt. A biometrikus azonosítás egyik legelterjedtebb megjelenési formája az ujjnyomat, ahogy egy korábbi bekezdésben is utaltam rá, jelen esetben egy holland munkahelyen, nyilvántartási célból került felhasználásra.[27] Mivel a GDPR a személyes adatok különleges kategóriái közé sorolja a biometrikus adatot, mint a természetes személyek egyedi azonosítását célzó adatot, így fokozottabb védelemben részesíti.[28] A rendelet főszabályként

[24] David Zhang – Guangming Lu: *3D Biometrics Systems and Applications*. New York, Springer, 2013. 283.

[25] Tóth i. m. 66–67.

[26] Anil K. Jain – Ajay Kumar: Biometric Recognition. In: Emilio Mordini – Dimitros Tzovaras: *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht, Springer, 2012. 49-54.

[27] Lojek Levente: *Bírság munkavállalók ujjlenyomatának indokolatlan kezeléséért*. https://bit.ly/39OJq1M [a továbbiakban: Lojek (2020a)]

[28] Péterfalvi–Révész–Buzás i. m. 72–73.

tiltja ezeknek az adatoknak a kezelését[29], illetve határozott feltételeket[30] társít a kezelésük mellé. Ezenkívül az adatkezeléshez mindig szükséges egy jogalap megléte[31], amely jelen esetben az adatkezelő szerint a munkavállalók önkéntes hozzájárulása volt.[32]

Felmerülhet itt bennünk a kérdés, hogy vajon mennyire tekintendő önkéntes a munkavállaló hozzájárulása ilyen esetben? Valószínűleg semennyire, ugyanis egy olyan helyzetről beszélünk jelen esetben, ahol a munkavállaló és a munkáltató alá-fölérendeltségi viszonyban állnak, így feltételezhető, hogy ilyen esetben a munkavállaló nem fog ellentmondani a munkáltatójának.[33] A munkáltatói oldal malmára hajtja a vizet az is, hogy tisztában van azzal a ténnyel, hogy nyomás és megfelelő szavak, netán ígéretek hatására a munkavállaló rendelkezésre fogja bocsátani az adatait önként, azonban ilyen esetben már nem beszélhetünk a GDPR szerinti tényleges önkéntességről.

A másik probléma pedig az lehet, hogy még ha el is fogadjuk azt az állítást, hogy egyes munkavállalók valóban önkéntesen járultak hozzá az adataik kezeléséhez, akkor is biztosak lehetünk abban, hogy van egy olyan csoport, akik nem kívánják semmiféleképpen a biometrikus adataikat átadni az adatkezelőknek. Ebben az esetben őket sem érheti hátrány a munkavégzésben, így a munkáltató köteles lenne nekik biztosítani egy alternatívát, amellyel élni tudnak.[34] Ez esetben meglátásom szerint, ha az előző problémával összekapcsoljuk az ügyet, akkor megvalósítható lenne az, hogy egyesek, tényleges önkéntes alapon válnak adatkezelés alanyaivá, míg mások az önkéntes hozzájárulást megtagadva, egy másik megoldás révén kerülnek be a nyilvántartásba.

A GDPR alapelvei szerint az adatkezelés alapelvei közül jelen esetben az adatkezelő megsértette a célhoz kötöttség elvét és az adattakarékosság elvét is. Az adatkezelési tevékenység célja a munkavállalók nyilvántartása, jelenléti ív ellenőrzése volt, így a DPA álláspontja szerint nem volt indokolt a szenzitív adatok kezelése, ugyanis ezen adatkezelési cél más módon, különleges személyi adatokat nem felhasználva is sikeresen megvalósítható lett volna. Kimondta a hatóság, hogy az ujjnyomat kezelése vagy önkéntes hozzájárulás alapján vagy valamilyen adatbiztonsági célból lett volna indokolt, melyhez a hatás-

29 GDPR 9. cikk (1) bekezdés.

30 Uo.

31 GDPR 6. cikk (1) bekezdés.

32 Lojek (2020a) i. m.

33 Uo.

34 Lojek (2020a) i. m.

vizsgálat elkészítésének eredménye után hivatkozhatott volna az adatkezelő.[35] Véleményem szerint azonban az önkéntes hozzájárulás jelen esetben nem állta volna meg a helyét, ugyanis a korábbi gondolatomra visszakanyarodva, miszerint a munkáltató és a munkavállaló között nem azonos szintű viszonyról beszélünk, kiemelném, hogy nehezen lett volna a teljes mértékű önkéntesség bizonyítható az adatkezelői oldalról.

5.2. A spanyol hatóság állásfoglalása

A pandémia által okozott hirtelen változások a társadalom minden szereplőjének életét érintették, ugyanis nem csak a munkahelyeken váltottak home office munkavégzésre a munkavállalók, hanem a diákok is távoktatásban kellett, hogy folytassák tanulmányaikat. A következő eset Spanyolországban, e változás következtében jelent meg. A Spanyol Adatvédelmi Hatóság (továbbiakban: AEPD) 2020. május 8-án egy jelentést adott ki, amely a biometrikus azonosítás jogszerűségének vizsgálatát tartalmazta. A tényállás szerint, a karanténhelyzet miatt az oktatók úgy próbálták meg azonosítani a diákokat az vizsgákon való részvételkor, hogy arcfelismerő rendszert használtak. Az AEPD álláspontja szerint a koronavírus okozta helyzet sem indokolja azt, hogy egyes alapjogok megsértése elfogadhatóvá váljon a cél elérése érdekében, így az adatkezelők az adatkezelési tevékenység folytán továbbra is kötelesek a GDPR rendelkezéseinek megfelelően eljárni. Jelen esetben az előző példához hasonlóan felmerül a kérdés bennünk, hogy mennyire fogadható el az érintettek beleegyezése önkéntes hozzájárulásként? Abban az esetben, ha a diákok nem egyeznek bele a biometrikus adatkezelésbe, hátrány éri őket a többiekkel szemben, ugyanis megvonják maguktól a vizsgázási lehetőséget.[36] Álláspontom szerint az ezen alapuló megkülönböztetés jellege diszkriminatívnak is minősül ebben az esetben, ugyanis ugyanazon egyetemre járó diákok ugyanazon kötelezettségüknek azért nem tudnak eleget tenni, mert nem járulnak hozzá a szenzitív adataik rendelkezésre bocsájtásához. Illetve a kérdés még itt az, hogy mennyire indokolt biometrikus adatgyűjtés végzése a vizsga lefolytatásához? Véleményem szerint itt a szükségesség követelménye nem valósul meg, ugyanis más módon is lehetséges lenne az azonosítás elvégzése. További probléma, hogy az előző

[35] Lojek (2020a) i. m.

[36] Lojek Levente: *Használható-e az arcfelismerés a diákok azonosítására?* https://bit.ly/3oAWSuj (letöltve: 2020.10.20.) [a továbbiakban: Lojek (2020b)]

esethez hasonlóan az érintettek itt is nyomás alatt állnak az adatuk megadásakor és erre az AEPD is rámutatott jelentésében. Állásfoglalása szerint, nem részesülhet hátrányban egyik diák sem amiatt, mert nem kívánja rendelkezésre bocsájtani valamely biometrikus adatát. Az előzőekhez hasonlóan itt is kiemelte, hogy fontos egy olyan alternatívát is biztosítani, amely lehetőséget ad azoknak, akik megtagadják az adatkezelési tevékenységben való érintettként történő részvételt.[37] A hatóság kihangsúlyozta, hogy az önkéntes hozzájárulás teljes mértékű megvalósulása esetén is a szükséges hatásvizsgálat elvégzése[38], valamint kockázatértékelés elvégzése következtében a felügyeleti hatósággal való konzultáció sem maradhat el az arcfelismerő azonosító rendszerek bevezetését megelőzően.[39]

5.3. A lengyel hatóság közleménye

A holland példához nagyon hasonló módon, Lengyelországban is született egy közlemény, amelyet a Lengyel Adatvédelmi Hatóság (továbbiakban: UODO) 2020. május 11-én adott ki. Ebben az esetben az első példához hasonlóan a munkavállalók munkaidejének nyilvántartásához szükséges biometrikus adatok kezelését utasította vissza a hatóság.[40]

Ahogy a korábbiakban is láttuk, a hatóság itt is kiemelte, hogy a biometrikus adatkezeléssel zajló tevékenység akkor jogszerű, ha megfelel egy GDPR szerinti jogalapnak[41] illetve, ha egy benne foglalt kivétel is társul mellé a felsoroltak közül[42]. Munkajogi probléma esetén azonban az adott ország munkajogi jogszabályait sem szabad figyelmen kívül hagyni. Ezen szabályok tartalmának betartása mellett szükséges a GDPR rendelkezéseit követni, azonban a lengyel munkaügyi törvény nem tartalmaz olyan rendelkezést, amely jelen esetben engedélyezné a biometrikus adatkezelési tevékenység végzését a munkaidő nyilvántartása és ellenőrzése céljából. Az UODO a továbbiakban kiemeli azt, hogy mindaddig, amíg a munkáltatónak más eszközei is vannak arra, hogy

---

37 Lojek (2020b) i. m.

38 GDPR 35. cikk

39 Lojek (2020b) i.m.

40 Lojek Levente: *Lengyelország: A munkaidő nyilvántartására nem használható biometrikus adat*. https://bit.ly/3lK3ynP [a továbbiakban: Lojek (2020c)]

41 GDPR 6. cikk (1) bekezdés.

42 GDPR 9. cikk (2) bekezdés.

ellenőrizze a dolgozókat és a munkaidőjüket, addig nem felelhet meg a szükségesség elvének a szenzitív adatkezeléssel járó nyilvántartás.[43]

Összegezve a három európai esetet megállapíthatjuk, hogy a biometrikus adatkezeléssel járó tevékenység végzése nagyon szigorú szabályokhoz kötött, ugyanis a biometrikus adat megmásíthatatlanságából fakadóan különös védettséget élvez. Az európai joggyakorlat arra hívja fel az adatkezelők figyelmét, hogy amíg van más járható út az azonosításra, addig nem indokolt a biometrikus azonosítás használata, csak, ha ténylegesen minden alapelvnek megfelel az adatkezelés és, ha megvan a megfelelő jogalap, illetve a rendeletben foglalt kivételek valamelyike fennáll.

5.4. Magyarországon megjelenő gyakorlat

Eddig a nemzetközi döntéseket vizsgálva ismertettem a biometrikus adatok azonosítás céljából történő használatának jogszerűségét, most azonban specifikusan a magyar gyakorlaton keresztül szemléltetném a téma aktualitását. Hazánkban is egyre elterjedtebb már a biometrikus azonosítórendszerek használata és az évek előre haladtával egyre inkább gyakoribb lesz. A Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) az elmúlt évek során egyre több döntést hozott a témában, amelyek közül a legismertebbet szeretném vizsgálni.

A vénaszkenner alapú biometrikus azonosítórendszer megjelenése hosszas vitákat okozott a hazai törvényalkotásban, ugyanis az első jelentős lépést a biometrikus azonosítás területén a Ferencvárosi Torna Club futball mérkőzéseire való belépést ellenőrző rendszer hozta. Az említett sportegyesület mérkőzésein az elmúlt években csak úgy van lehetőség részt venni, ha a szurkolók a szurkolói kártyájuk megvásárlásakor vénalenyomatot is adnak a szervezőknek. Erre azért van szükség, mert a mérkőzésekre való belépéskor a szurkolói kártya és a vénalenyomat leolvasása alapján azonosítják az érkező vendégeket. Mindehhez hozzátársulnak még további feltételek, ugyanis a mérkőzést megelőzően szükséges előzetesen leadni az érintettek nevét, születési adatát, képmását és hozzá kell járulniuk a vénanyomatuk rögzítéséhez.[44]

---

[43] Lojek (2020c) i. m.

[44] Szabó Máté Dániel: *Vénaszkenner az FTC pályán, biometrikus adatok az AB ülésein*. https://bit.ly/2JScSJl

A vénaszkenner bevezetéséről folyó viták közvetlen előzménye az Stv. T/156. számú törvényjavaslattal történő módosítása volt. A NAIH az Infotv.[45] 38.§ (4) bekezdés a) pontjában meghatározott jogszabály-véleményezési feladatkörét ellátva észrevételeket nyújtott be a törvénymódosítással kapcsolatban. Ebben az állásfoglalásban a NAIH szigorú követelményeket fogalmazott meg a módosításokkal kapcsolatban. Itt szerepelt először a biometrikus azonosítórendszer bevezetésének gondolata a futball szurkolók azonosítása céljából. A törvényjavaslat 2.§ szerint a törvény részét képezi majd az, hogy a klubkártyával rendelkező egyénektől a szervezők valamely biometrikus adatot kezeljenek személyazonosítás céljából. A NAIH fontosnak tartotta, hogy a szükségesség elvének megfelelve bebizonyosodjon, hogy a rendszer használata nem mellőzhető, mindemellett a tevékenység céljának eléréséhez hatékony segítséget nyújt. A NAIH ebben az esetben is hangsúlyozta, hogy biztosítani kell más alternatívát is a cél elérése érdekében és, ha annak segítségével ugyanúgy elérhető az, akkor azokat kell előnyben részesíteni.[46]

Ezt követően alkotmányjogi panaszt nyújtott be az egyik érintett, alapjogsérelemre hivatkozva, amely őt érte a vénaszkenner alkalmazása során. A panaszban előadta, hogy bérletvásárlás során a fent említett feltételeket teljesítenie kellett, így adatkezelés alanyává is vált, különös figyelmet szentelve a szenzitív adatának kezelésére. Álláspontja szerint a vénalenyomat rögzítése szükségtelen és aránytalan is egyben, amelynek következtében jogaiban elfogadhatatlan mértékben korlátozottá válik az érintett. Panaszában kitért rá, hogy véleménye szerint a magánszféra védelméhez való jogát[47] és az információs önrendelkezéshez való jogát[48] is sérti a biometrikus azonosítórendszer alkalmazása. Ezen jogsértés pedig úgy valósult meg, hogy aránytalan és szükségtelen módon korlátozódtak az érintett alapjogai.[49]. A panaszában az érintett arra tért ki, hogy az Alaptörvény szerint nem feleltethető meg a biometrikus adat kezelése, ugyanis a rendszer használatával korlátozva vannak az őt érintő alapjogok, de nem felelnek meg a szigorú feltételeknek. Utolsó pontként pedig sérelmezte az érintett azt, hogy a hozzátartozó biometrikus adatot nem a sportkártyáján, hanem egy

[45] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[46] A Nemzeti Adatvédelmi és Információszabadság Hatóság elnökének NAIH/2015/4674/2/J számú véleménye a sporttörvény módosításáról

[47] Ld. Magyarország Alaptörvénye VI. cikk (1) bekezdés.

[48] Ld. Magyarország Alaptörvénye VI. cikk (2) bekezdés.

[49] Ld. Magyarország Alaptörvénye I. cikk (3) bekezdés.

egységesített adatbázisban tárolják, amely eredményeképpen az önrendelkezési jogát sérti a rendelkezés.[50]

A vénaszkenner ügyét ezt követően háromszor tárgyalta az Alkotmánybíróság és kilenc kérdésben a NAIH szakmai véleményét is kikérte a témában.

Összességében megállapíthatjuk, hogy a vénaszkenner bevezetése nagy problémát okozott Magyarországon, ugyanis több érintett is alapjog-sérelemre hivatkozva panaszt nyújtott be ezzel kapcsolatban az Alkotmánybírósághoz. Ennek ellenére még nem született döntés az ügyben a bíróság által, a NAIH azonban a Stv. és az adatvédelmi jogszabályokra hivatkozva megfelelőnek tartja a rendszer létrejöttét, amely azóta is működik a Groupama Arénában. A Stv. rendelkezései szerint lehetséges az ilyen jellegű azonosítás, így a NAIH véleményében ettől nem tud eltérni, ugyanis törvényi rendelkezés tartalmazza a rendszer használatát, csupán felhívja a figyelmet arra, hogy a biometrikus adattal működő rendszerek esetén milyen szintű védelem szükséges az adatok megőrzésekor.[51] Azt azonban nem szabad szem elől tévesztenünk, hogy a vénaszkenner bevezetésekor a GDPR még nem volt hatályban, így az akkor hatályban lévő Stv. szerinti rendelkezések voltak irányadók.

Mind ezek mellett a NAIH már egyéb esetekben is foglalt állást a biometrikus azonosítórendszerek használatával kapcsolatban. Egyik esetben például, egy magánszemélytől érkező bejelentés alapján vizsgálta az esetet, amelyben a Semmelweis Egyetem ÁOK Szemészeti Klinika ujjnyomat alapú biometrikus beléptetőrendszer vezetett be a munkaidő nyilvántartás ellenőrzése céljából. A hatóság, a nemzetközi döntésekhez hasonlóan, itt is megállapította, hogy a célszerűség elvének nem feleltethető meg az adatkezelés, kiváltképpen azért, mert más módon is lehetséges a munkaidő ellenőrzése, biometrikus adathasználat nélkül. Álláspontja szerint, az Mt.[52] is tartalmaz olyan lehetőséget, amely alternatívaként használható lenne ebben az esetben.[53]

Végül megállapítható, hogy a NAIH a biometrikus azonosítórendszerek bevezetésének esetében szigorúan figyelemmel kíséri az alapelveknek való megfelelőséget és legtöbb esetben megtiltja a rendszer bevezetését a szükséges cél megfelelőségének hiányában.

---

50 A Társaság a Szabadságjogokért anonim alkotmányjogi panasza a vénaszkenner ügyében. https://bit.ly/2L7QWdz

51 Szabó i. m.

52 Ld. a Munka Törvénykönyvéről szóló 2012. évi törvény 134.§ (3) bekezdés.

53 A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről. 34 – 35. https://bit.ly/3uWMvVg

6. Összegzés

Megállapítható, hogy az adatvédelmi jog és a biometrikus adatok, valamint biometrikus azonosítórendszerek igencsak sok kérdést vetnek fel gyakorlati alkalmazásuk során. Általánosan elmondható, hogy nem csupán hazánkban, hanem a nemzetközi gyakorlatban is komoly jogértelmezési kérdések elé állítja az adatvédelmi hatóságokat. Mivel az elmúlt évekre visszatekintve nincs még kialakult joggyakorlat a területen, így lényegesen több egyeztetés és állásfoglalás során lehetséges a gyakorlatban megjelentetni a biometrikus azonosítórendszereket.

Fontos azonban kiemelni azt, hogy a technológia fejlődésének köszönhetően a biometrikus azonosítórendszerek alkalmazási területe is kiszélesedett. Ennek következtében a magánszféra is érintetté vált a rendszer működése során, aminek köszönhetően adatvédelmi aggályokat vetett fel a gyakorlati megjelenés. A bemutatott európai jogesetekre fókuszálva megállapítható, hogy a hatóság minden esetben szigorú kereteket adott a gyakorlati megjelenés esetén a megfeleltethetőség kérdésében. Akár a külföldi viszonylatot nézzük, akár a hazait, megállapítható, hogy az adatvédelmi hatóságok még kevés olyan esettel találták szemben magukat, ahol a biometrikus azonosítórendszerek jogszerű működése elfogadható lett volna. Általában valamely GDPR adta alapelv követelményeibe ütközött az adatkezelési tevékenység, legtöbbször a célhoz kötöttség elvébe. Ennek alapját a legtöbb esetben az adta, hogy azért nem volt elfogadható a rendszer működtetése, mert más alternatív módon is lehetséges lett volna az adatkezelési tevékenység céljának elérése, amely kevesebb lehetséges érdeksérelemmel járt volna. A hatóság minden esetben azt hangsúlyozta, hogy mivel a biometrikus adat szenzitív adat, így kezelése csak kivételes esetekben elfogadható.

A kérdés, amely a kutatómunkám során megfogalmazódott bennem az volt, hogy indokolt-e ennyire körül bástyázni ezen adatok kezelését? Ennek fényében arra a megállapításra jutottam, hogy bírálom azt, hogy Európában az adatvédelmi szabályozás ennyire szigorú a biometrikus azonosítás bevezetése esetén. Megállapításaim szerint, a technológia fejlődésének következtében egyre inkább indokolt lesz az emberek azonosításának fejlődése, gyorsítása, automatizálása is. Nem lesz elfogadható az, hogy a technológia fejlődése sokkal előbbre jár már, de a jogszabályok által szabott keretek miatt ezen újítások nem valósíthatók meg idővel sem a mindennapjaink során. Ezen kívül a közérdeket is szolgálná, ha a jogrendszer engedélyezné a technológia fejlődések létrejöttét, megvalósulását. Abban az esetben, ha a technológia megfelelően biztonságban tudná kezelni a biometrikus adatokat és az adatkezelők is felmérnék azt, hogy

milyen súlya van valójában a különleges adatok kezelésének, akkor a jogszabályoktól is elvárható lenne, hogy lazább keretet szabjanak a biometrikus azonosítás megvalósításának. A társadalom mozgatórugója ugyanis örökké a technológia fejlődése lesz és az egyéneknek ehhez kell majd igazodniuk az élet összes területén. Mindehhez elengedhetetlen az is, hogy a jogszabályok is lépést tartsanak a technológiai újításokkal, hogy határokat tudjanak szabni azok működésének.

A biometrikus adat különleges személyes adat létének köszönhetően fokozott védelemben részesül. A megmásíthatatlanságából kifolyólag az emberi lét ideje alatt végig egyénhez köthető, így álláspontom szerint, csak olyan esetekben fogadható el a használata, ahol megfelelő érdek és biztonsági faktor kötődik a tevékenység végzéséhez. Mivel ennek elvesztése, eltulajdonítása esetén aránytalanul nagy sérelem éri az érintettet, így egyetértek abban, hogy fokozottan védeni kell és mérlegelni azt, hogy mennyiben indokolt a használata. Javaslatom szerint, így egy magas biztonsági keretek között zajló tevékenység végzéséhez, akár egy laboratóriumban, akár egy kórházban, ahol az egyéni érdeket is szolgálja a pontos azonosítás megléte, lehetővé kellene tenni az azonosítórendszerek használatát. Ehhez társítva követelményként egy évenkénti ellenőrzést javasolnék, amely biztosítaná azt, hogy az azonosítás céljának indokoltsága végig ellenőrizve legyen, és az adatok más célból történő, jogellenes felhasználása, kizárható legyen.