

JOGI FÓRUM PUBLIKÁCIÓ

Biometrikus adatok kezelése
Az ujjlenyomattal történő azonosítás adatvédelmi kérdései

Szerző:

dr. Holczknecht Zoltán LL. M.

bírsági titkár

digitális adatvédelmi szakjogász

Harkány, 2025. 11. 17.

Tanulmányomban a vonatkozó jogszabályok és szakirodalom segítségével bemutatom az ujjlenyomat, mint biometrikus azonosító adat munkahelyi használatának adatvédelmi és szükségképpen munkajogi követelményeit. Áttekintem a biometrikus adatokkal kapcsolatos legfontosabb fogalom meghatározásokat. Megvizsgálom az adatkezeléssel kapcsolatos alapelveket, az adatkezelés jogalapjait és adatkezeléssel kapcsolatos követelményeket, továbbá a NAIH ezzel kapcsolatos joggyakorlatát és külföldi jogesetet is bemutatok. Dolgozatomban érintőlegesen bemutatom továbbá a biometrikus adatok kezelésére vonatkozó, büntetőeljárás során alkalmazandó szabályokat, rávilágítva a két szabályozás eltéréseire.

1. Definíciók

Szükségnek látszik a dolgozat elején tisztázni a legfontosabb definíciókat a biometrikus adatokkal kapcsolatosan.

A biometria kifejezésnek több fogalmi magyarázata ismert, görög eredetű szó, amely az „élet” (bio) és a „mérés” (metria) szavakból áll. Olyan mérhető fizikai vagy biológiai jellemző, amely lehetővé teszi az egyén azonosítását. ¹

A „biometrikus adat” fogalmát az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (GDPR) 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 adatként határozza meg.²

A 29. cikk alapján létrehozott adatvédelmi munkacsoport által kiadott 4/2007 vélemény a személyes adat fogalmáról a biometrikus adat fogalmát a következőképpen határozza meg: „biológiai jellegzetességekként, viselkedési vonatkozásokként, pszichológiai sajátosságokként, életvitelként

¹KOVÁCS T. - MILÁK I. - OTTI Cs.: A biztonságstudomány biometriai aspektusai
<http://www.pecshor.hu/periodika/XIII/kovacsti.pdf>, (letöltve: 2024.11.14.) 1. oldal

²GDPR. 4. cikk 14. pont

vagy olyan ismétlődő tevékenységekként, amelyek során e jellegzetességek és/vagy tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is.”³ és ezen fogalmat tekinti alapnak munkacsoport 3/2012. sz. véleménye a biometrikus technológiák terén történt fejleményekről.

Fenti definíciókkal összhangban határozza meg a biometrikus adat fogalmát az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.) az értelmező rendelkezések között, mely szerint „biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat”⁴

A biometrikus adatok forrása: „a biometrikus adatok forrásai (például az emberi szövetminták) önmagukban nem tekinthetők biometrikus adatnak, de felhasználhatók biometrikus adatok gyűjtésére (az információ belőlük való kinyerése útján)”⁵

A biometrikus technikáknak két fő kategóriájuk van. - Egyrészt vannak fizikai és fiziológiai alapú technikák, amelyek a személyek fizikai és fiziológiai jellemzőit vizsgálják, ezek közé tartozik többek között és jellemzően az ujjlenyomat-ellenőrzés, az ujjkép-elemzés, az íriszfelismerés, a retinaelemzés, az arcfelismerés.

Másrészt vannak viselkedésen alapuló technikák, amelyek a személyek viselkedését mérik, ezek közé tartozik a kézzel írt aláírás ellenőrzése, a gépirás elemzése, a járás elemzése, a járásmód vagy a mozgás módja, a valamilyen tudatalatti gondolatra, például hazugságra utaló mintázatok stb.

³4/2007. sz. vélemény (WP136) letöltve: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf 9. old (letöltés ideje 2024. 11. 14.)

⁴ Info tv. 3. § 3b. pontja

⁵ 4/2007. sz. vélemény (WP136) letöltve: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf 9. old (letöltés ideje 2024. 11. 14.)

A „biometrikus adatkezelés”: Magában foglalja a biometrikus azonosítás során gyűjtött adatok kezelését, tárolását, feldolgozását és védelmét. GDPR a különleges személyes adatok körébe sorolja

6

2. Az ujjlenyomat alkalmazásának rövid történeti áttekintése

Az ujjlenyomat mint egyedi azonosítási eszköz története több ezer évre nyúlik vissza, azonban modern kriminalisztikai és igazgatási célú alkalmazása csak a 19. század második felétől indult meg. A legkorábbi ismert feljegyzések szerint már az ókori Babilonban, illetve a kínai császári adminisztrációban is használtak ujj- vagy tenyérlenyomatot hitelesítési célokra, elsősorban okiratokon és kereskedelmi megállapodásokon. Ezek az alkalmazások azonban nem tudományos jellegűek voltak, sokkal inkább gyakorlati megoldások a személyes beazonosítás megkönnyítésére.

A tudományos igényű ujjnyomat-vizsgálat kialakulása Sir William Herschel nevéhez kapcsolódik, aki 1858-tól Indiában, a brit közigazgatás szolgálatában kezdte rendszerszerűen alkalmazni az ujjlenyomatot szerződések hitelesítésére. Herschel felismerte, hogy az ujjnyomat egyedi és időben állandó, ám kutatásait ekkor még nem kriminalisztikai célból, hanem igazgatási funkció keretében végezte. A modern daktiloszkópia alapjait Francis Galton brit antropológus fektette le az 1890-es években, aki statisztikai módszerekkel igazolta az ujjlenyomatok egyediségét és változatlanságát, valamint kidolgozta első osztályozási rendszerét. Galton eredményei nyitották meg az utat az ujjlenyomat kriminalisztikai felhasználása előtt.

A tényleges bűnüldözési célú ujjnyomat-nyilvántartás bevezetése Henry Faulds és Edward Henry munkájához köthető. Henry fejlesztette ki azt az osztályozási rendszert, amely lehetővé tette a nagy mennyiségű ujjnyomat adat hatékony tárolását és visszakeresését. Ennek eredményeként a 20. század elejére több ország - köztük az Egyesült Királyság és az Egyesült Államok - rendvédelmi szervei hivatalosan is bevezették az ujjnyomatvételt a személyazonosítás és a bűnügyi nyilvántartás részévé. A technológiai fejlődés újabb mérföldkövet jelentett az automatizált ujjnyomat-azonosító rendszerek (AFIS - Automated Fingerprint Identification System) megjelenésével az 1980-as évektől kezdődően.

⁶ GDPR 9. cikk (1) bekezdés

Az AFIS lehetővé tette a nagyméretű ujjnyomat-adatbázisok elektronikus összehasonlítását, jelentősen gyorsítva a vizsgálati folyamatokat és növelve a kriminalisztikai pontosságot. A digitális feldolgozás révén az ujjnyomat ma már nem csupán egy kriminalisztikai eszköz, hanem számos igazgatási eljárás (pl. útlevelekibocsátás, határellenőrzés) alapvető eleme.

A 21. század elejére az ujjnyomat a világ egyik legelterjedtebb biometrikus azonosítási módszerévé vált. A fejlődést egyrészt a kriminalisztikai sikeresség, másrészt a digitális technológiák széles körű alkalmazása ösztönözte.

3. Ujjlenyomat használattal kapcsolatos adatvédelmi aggályok

Az ujjlenyomatok használatával kapcsolatos adatvédelmi aggályok a 3/2012. számú vélemény alapján röviden a következőképpen írhatók le:

- Pontosság: az ujjlenyomatok végső soron nagy pontosságú adatot eredményeznek. A rossz adatminőség vagy a nem következetes adatszerzési folyamat, továbbá a megjelenítés korlátai a pontosság rovására mennek.
- Hatás: a folyamat visszafordíthatatlansága csökkentheti az egyén azon lehetőségét, hogy gyakorolja a jogait vagy megváltoztassa a hamis azonosítás alapján meghozott döntéseket. A biztonsági intézkedések hiánya személyazonosság-lopáshoz vezethet, amely jelentős hatással lehet az egyénre.
- Összekapcsolhatóság: az ujjlenyomatok lehetőséget nyújtanak a visszaélésre, mivel az adatok összekapcsolhatók más adatbázisokkal. A más adatbázisokkal való összekapcsolás e lehetősége az eredeti célokkal össze nem egyeztethető felhasználást eredményezhet.
- Különleges adatok feldolgozása: néhány tanulmány szerint az ujjlenyomatok képei az egyénre vonatkozó etnikai információkat fedhetnek fel.⁷
- Az adatok központi tárolása - különösen nagy adatbázisokban - az adatbiztonsághoz, az összekapcsolhatósághoz és a funkciók terjeszkedéséhez kapcsolódó kockázatokkal jár. Ez

⁷ <http://fingerprints.handresearch.com/dermatoglyphics/fingerprints-world-map-whorls-loops-arches.htm> Martijn van Mensvoort MAY 11, 2011 [LAST UPDATES: MARCH, 2015] letöltve 2024. 11. 14.

biztosítékok hiányában lehetővé teszi az ujjlenyomatok olyan célokra való felhasználását, amelyek eltérnek a feldolgozást eredetileg indokoló céloktól.

- A hozzájárulás központi kérdés az ujjlenyomatok bűnüldözés területén kívül eső felhasználása terén. Az ujjlenyomatok könnyen lemásolhatók rejtett lenyomatokról vagy akár fényképekről is az egyén tudomása nélkül.
- Az ujjlenyomat-adatok időben kifejezetten állandók, és megmásíthatatlannak tekintendők. Ujjlenyomat-sablon bizonyos feltételekkel azonban megmásítható.
- Csalás elleni védelem: az ujjlenyomatok könnyen gyűjthetők, mert egy egyén több ujjlenyomatot hagy hátra. Ráadásul a hamis ujjlenyomatok sok rendszer és érzékelő esetében felhasználhatók, különösen, ha az ilyen rendszereknek nem képezi részét külön csalás elleni védelem.⁸

4. Alapelvek és jogalapok

Nem lehet a különleges adatok kezelésének követelményeit megvizsgálni anélkül, hogy ne említenénk az adatkezelés általános elveit, melyekkel a NAIH által 2026-ban kiadott tájékoztató részletesen foglalkozik. Az irányadó a korábban már említett WP29 Munkacsoport 3/2012. számú véleménye, mely egyértelműen meghatározott adatvédelmi követelményeket fogalmaz meg, melyeknek érvényesülnie kell, hogy az adatkezelés, konkrétan a biometrikus adatkezelés jogszerűnem minősüljön.

4.1. Az adatkezelés alapelvei

Minden adatkezelés során érvényesülő alapelv a jogszerűség, tisztességes eljárás és átláthatóság. Ezen alapelv általános jelleggel követeli meg a jogszabályok tiszteletben tartását és feltételezi a jogalapot, ahogy azt a GDPR Preambulum is rögzíti a 40. bekezdésben „Annak érdekében, hogy a személyes adatok kezelése jogszerű legyen, annak az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított - akár e rendeletben, akár más, az e rendeletben említettek szerinti uniós vagy tagállami jogban foglalt - alappal kell rendelkeznie,

⁸ 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről letöltve https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf (letöltés ideje 2024. 11. 14.)

ideértve az adatkezelőre vonatkozó jogi kötelezettségeknek való megfelelés szükségességét, az érintett által kötött esetleges szerződés teljesítését, illetve az érintett által kért, a szerződéskötést megelőzően megteendő lépéseket.” Az adatkezelésnek továbbá a teljes folyamat alatt meg kell felelnie a tisztesség és átláthatóság követelményének.

A célhoz kötöttség elve alapján személyes adatot csak előre meghatározott célból lehet kezelni, azaz minden esetben meg kell vizsgálni, hogy a biometrikus adatok kezelése valóban elengedhetetlen-e az elérni kívánt célhoz, vagy esetleg erre kizárólag költséghatékonyság vagy kényelem miatt kerül sor. Vizsgálandó, hogy a biometrikus adatok kezelésének előnyei arányban állnak-e az érintettek jogainak korlátozásával. Elvárás, hogy az adatkezelő összevesse a biometrikus adatok kezelésének hatékonyságát más, kevesebb adatkezelést, vagy nem különleges adat kezelését igénylő módszerrel, mely során szükséges annak felmérése, hogy a cél elérhető-e más, az érintett magánszférájában kevésbé beavatkozó módszerrel. Ezen alapvetően a NAIH is következetesen képviseli állásfoglalásaiban. A célhoz kötöttség elvének alapvető elemei a konkretizálás, azaz a célt még az adatok gyűjtése előtt meg kell határozni. Elengedhetetlen a jogosultság, az adatkezelés céljának jogszerűnek kell lennie és csak olyan célra gyűjthetők, melyeket a GDPR vagy más jogszabály engedélyez. A biometrikus adatok, úgy az ujjlenyomat kezelése során figyelemmel kell lenni arra, hogy különleges adatnak minősül, melynek kezelését a GDPR fő szabály szerint tiltja. A célhoz kötöttséget az adatkezelés teljesen időtartama alatt fenn kell tartani, azaz az adatot csak addig lehet kezelni, míg annak kezelése az adatkezelés során meghatározott célt szolgálja, új célra felhasználni csak az érintett tájékoztatása és új jogalap biztosítása mellett lehet. Ezen követelmények alóli kivétel az érintett hozzájárulása vagy amennyiben az új cél összhangban van az eredetivel.

Az adat takarékoság és alapértelmezett adatvédelem elve alapján csak a cél megvalósításához feltétlenül szükséges mértékben, a célhoz kötöttség elvével szoros összefüggésben meghatározza az adatkezelés terjedelmi és időbeli korlátját is, csak annyi adat kezelhető, amennyi szükséges és elégséges az adatkezelés céljának eléréséhez. Ezen alapelvekkel szorosan függ össze a korlátozott tárolhatóság elve, azaz csak a cél megvalósulásáig lehet a személyes adatot kezelni, a jogszabályban meghatározott kivételekkel.

A pontosság elve az adatok pontos kezelését jelenti, figyelemmel arra, hogy azok időszerűek és naprakészek legyenek. A kezelt adatoknak pontosaknak és hiánytalanoknak kell lennie, különösen a személyes adatok felvételénél kell az adatkezelőnek kiemelt figyelmet fordítania a precíz adatrögzítésre. Az adatok pontosságának elve azonban nem feltétlenül jelenti azt, hogy az adatoknak objektíve tükrözniük kell a valóságot, inkább azt jelenti, hogy az adatkezelés célja megvalósulásának érdekében relevánsnak, jól megválasztottnak kell lenniük.

A korlátozott tárolhatóság elve alapján szintén fentebb részletesen kifejtett alapelvekkel összhangban az adatokat csak a cél megvalósulásáig lehet kezelni.

Az integritás és bizalmas jelleg elve alapján a személyes adatokat olyan módon kell kezelni, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását. A technológia fejlődésével ezen alapelv érvényesülése különös jelentőséggel bír, hiszen egy adatvédelmi incidens nagy számú, az adatkezelő által kezelt, akár különleges adat is érinthet és ennek az érintettek életére beláthatatlan következménye lehet.

A biometrikus adatok egyedi, biztonságos kezelésük érdekében szigorúbb követelményeknek kell érvényesülnie. A WP29 Munkacsoport véleményében is felhívja a figyelmet, hogy a biometrikus adatok központosított tárolása megnöveli mind annak a kockázatát, hogy a biometrikus adatokat kulcsként használják több adatbázis összekapcsolásához (ami azt eredményezheti, hogy részletes profilt hoznak létre az egyénről), mind az ilyen adatok nem megfelelő célokra való újbóli felhasználásának sajátos veszélyeit, különösen engedély nélküli hozzáférés esetében. ⁹

Az elszámoltathatóság elve magába foglalja az adatkezelés tervezésétől annak folytatásán át a cél megvalósulásáig tett valamennyi lényegi lépés adminisztrálását, és egyben az adatvédelmi követelményeknek való megfelelés igazolására való képességet feltételezi. Szabályszerű és transzparens eljárást követel meg az adatkezelőtől. Az elv a gyakorlatban az adatkezelő számára a

⁹ 3/2012. sz. vélemény

GDPR-ban előírtaknak megfelelő tájékoztatók, szabályzatok, eljárásrendek szakszerű rögzítését és ezek megismerhetőségének biztosítását irányozza elő.

4.2. Adatkezelési jogalapok a GDPR rendelkezései alapján.

Az általános alapelvek után fontos megemlíteni az, hogy az adatkezelés jogszerűségéhez legalább az alábbi jogalapok egyikének fennállása szükséges:

- a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
- f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.¹⁰

4.3. A GDPR és Info tv. viszonya

Személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére az Info. tv.-t törvényt kell alkalmazni, vagyis ilyen esetekben csak a magyar jogi előírások alapján kell az adatkezelőnek eljárnia.¹¹ Ezen céloktól eltérő az adatkezelés a GDPR előírásai alkalmazandók.

¹⁰ GDPR 6. cikk

¹¹ Info tv. 2.§ (3) bekezdés

Tekintettel a speciális alkalmazásra, az esetek nagy jelentős részében egyértelműen meghatározható, hogy egy adott adatkezelés során melyik jogszabályt kell alkalmazni.

Ami kérdést vethet fel, az egy hogy fő tevékenységként az Info tv. hatálya alá tartozó adatkezelést végző szervezet azon adatkezeléseinek meghatározása, amelyek nem az Info. tv. hatálya alá esnek. Egy adott célból végzett személyes adat kezelés egyidejűleg nem tartozhat mind a GDPR, mind az Info. tv. hatálya alá, ugyanis az Info. tv. megfogalmazásából következően ha egy adatkezelés célja az Info. tv.-ben rögzített bűnüldözési, nemzetbiztonsági vagy honvédelmi cél, akkor csak az Info. tv. 5. §-ban meghatározott valamely jogalapon nyugodhat és az Info. tv. előírásai követendők, ha pedig nem ilyen célú az adatkezelés, akkor a GDPR 6. cikk (1) bek.-ben rögzített valamely jogalapja. Ebben az esetben nyilvánvalóan az adatkezelés célja határozza meg az alkalmazandó jogszabályt. Ha a cél az Info tv.-ben meghatározott cél, abban az esetben nyilvánvalóan az Info tv. rendelkezései az irányadóak, ha pedig az adott szervezet munkavállalóinak a nyilvántartásáról van szó, mellyel kapcsolatos adatkezelés nem az Info tv.-ben meghatározott céllal történik, abban az esetben a GDPR rendelkezéseit kell alkalmazni és ezen követelményeknek kell megfelelnie az adatkezelőnek.

5. A GDPR rendelkezése a különleges személyes adatokról

Az általános alapelvek és jogalapok tisztázása után térhetünk rá a különleges személyes adatok kezelésével kapcsolatos követelményekre.

A GDPR rendelkezése szerint a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.¹²

A GDPR 9. cikke szerint tehát a biometrikus adat különleges személyes adatnak tekinthető és annak kezelése főszabály szerint tilos. A GDPR 9. cikk 2. bekezdése felsorolja azokat a kivételeket, melyek

¹² A GDPR 9. cikk (1) bekezdése (1)

szerint az általános tiltás ellenére ezen adatok mégis kezelhetők. A dolgozat tárgya szempontjából a 2. bekezdés b) pontja lényeges, mely szerint az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi¹³

¹³ GDPR 9. cikk 2. bekezdés b) pont

6. A biometrikus adatok jogszerű kezelésének követelményei a hazai jog alapján

Hazánkban az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról szóló 2019. évi XXXIV. törvény, (GDPR „salátatörvény”) melyet az Országgyűlés 2019. április 1. napján tartott ülésén fogadott el, módosította a munka törvénykönyvéről szóló 2012. évi I. tv. (Mt.) adatkezeléssel kapcsolatos rendelkezéseit és a GDPR-ral összhangban meghatározta azokat a kivételes eseteket, amelyek esetén a munkáltató a munkavállalók biometrikus adatait az érintett azonosítása céljából kezelheti.

A módosításnak köszönhetően a biometrikus azonosító rendszerekkel kapcsolatban a biometrikus adatok kezelésének viszonylatában az Mt. sokkal komolyabb feltételeket támaszt.

Az Mt. általában is szigorú szabályokat határoz meg a munkavállaló adatainak kezelésével kapcsolatosan, így a munkáltató a munkavállalótól olyan nyilatkozat megtételét vagy személyes adat közlését követelheti, amely a munkaviszony létesítése, teljesítése, megszűnése (megszüntetése) vagy e törvényből származó igény érvényesítése szempontjából lényeges.¹⁴

A munkavállaló biometrikus adatainál azonban még szigorúbb követelményeket támaszt a jogszabály, ugyanis biometrikus adat az érintett azonosítása céljából abban az esetben kezelhető, ha ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy törvényben védett jelentős érdek súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna.¹⁵

A jogszabály egyértelműen felsorolja mik tekinthetők jelentős érdeknek, úgymint a legalább „Bizalmas!” minősítési szintű minősített adatok védelméhez, a lőfegyver, lőszer, robbanóanyag őrzéséhez, a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez, a nukleáris anyagok őrzéséhez, a Btk. szerint legalább különösen nagy vagyoni érték védelméhez fűződő érdek.¹⁶

¹⁴ Munka Törvénykönyvéről szóló 2012. évi I. tv. 10. §.

¹⁵ Munka Törvénykönyvéről szóló 2012. évi I. tv 11. §. (1) bekezdés

¹⁶ Munka Törvénykönyvéről szóló 2012. évi I. tv 11. §. (2) bekezdés

7. Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) álláspontja

A dolgozat témája szempontjából lényeges két NAIH dokumentumot szükséges megemlíteni, mindkettő a GDPR „salátatörvény” elfogadását megelőzően keletkezett, hatásuk azonban nyilvánvaló.

7.1.NAIH tájékoztató a munkahelyi adatkezelések alapvető követelményeiről

A korábban keletkezett NAIH tájékoztató 2016. október 28. napján kelt, és mely a céljának megfogalmazása szerint azért jött létre, hogy útmutatóul szolgáljon mind a munkavállalók, mind a munkáltatók számára, és megismerjék, hogy a munkavégzést érintő adatkezelések, különösen a munkáltatói ellenőrzéssel összefüggő adatkezelések esetében milyen követelményeknek kell érvényesülniük. A Hatóság a tájékoztatóban szereplő alapvető szempontokkal kívánja segíteni az adatkezelőket a jogszerű adatkezelés kialakításában.¹⁷

Az ajánlás az Adatvédelmi Munkacsoport 3/2012. számú véleménye alapján megadja a biometrikus adatok - jelen dolgozatomban is már említett - két kategóriáját, továbbá a biometrikus rendszerekkel kapcsolatos definíciókat. Kifejti továbbá - szintén a 3/2012. számú vélemény- alapján a biometrikus rendszerek alkalmazásával kapcsolatos követelményeket. Az ajánlás szerint mérlegelni kell, hogy a rendszer szükséges-e, azaz használata elengedhetetlen, elég hatékony lesz-e tekintettel az alkalmazni kívánt biometrikus technológia sajátos jellemzőire, továbbá arányos-e az elvárt előnyökkel, ha a rendszer miatt sérül a magánélet védelme. Meg kell továbbá fontolni, hogy más, a magánéletben kisebb mértékben beavatkozó módszerekkel nem lehet-e elérni a kívánt célt.¹⁸

Az ajánlás nem zárja ki a biometrikus rendszer alkalmazhatóságát, amennyiben fenti követelményeknek megfelel, megemlítve a Munkacsoport 6/2024. számú véleményében hozott példát a halálos vírusokkal dolgozó laboratóriumot.¹⁹ Ezzel teljes mértékben összhangban van a fentiekben már kifejtett Mt. módosításban felhozott kivételek közül a biológiai anyagok őrzése.

¹⁷ A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről 1. oldal

¹⁸ A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről 35. oldal

¹⁹ 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról letöltve https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf (letöltés ideje 2024. 11. 14.) 43. oldal

7.2.NAIH 2019/1074 számú ügyben adott tájékoztatója

A 2019. januárjában kiadott tájékoztató megállapítja, hogy általánosságban a munkahelyi adatkezelések, így a munkavállalók biometrikus adatai esetében a joggyakorlat nem változik a tekintetben 2018. május 25. követően sem, hogy erős függelmi viszonyokban a hozzájárulás jogcím főszabály szerint nem alkalmazható a személyes adatok kezelésére. Ezen megállapítás nyilvánvalóan a GDPR hazai hatályba lépésére vonatkozik, ugyanakkor megemlítendő, hogy a GDPR saláta törvény T/4479. számú javaslata 2019. februárban került benyújtásra.²⁰

A tájékoztató megállapítja, hogy az érintett hozzájárulása tipikusan nem képezheti az adatkezelés érvényes jogalapját erős függelmi jogviszonyokban. Ugyanezen okból a munkaszerződésbe vagy kollektív szerződésbe foglalt biometrikus adatszolgáltatási kötelezettség sem jogszerű, és egyébként ez az adatkezelés a munkaszerződés teljesítéséhez nem is feltétlenül szükséges.

Egyes kivételes esetekben azonban, ha a hozzájárulás szabadon és következményektől mentesen megtagadható, továbbá, ha a hozzájárulás nem a munkaviszony fenntartásának feltétele, akkor az adatkezelés jogalapjául az érintett hozzájárulása is szolgálhat.

Ha a hozzájárulás nélkül az érintett munkaviszonya megszűnik vagy terhesebbé válik, valamely előnytől esik, vagy egyéb hátrányt szenved el, akkor a hozzájárulás érvénytelen az akaratképzés szabadságának hiánya miatt.

A tájékoztató szerint, ha a fenti kivételes feltételek nem állnak fenn, akkor a GDPR 6. cikkének egyéb jogalapjai, elsősorban az (1) bekezdés f) pont szerinti jogalap jöhet szóba a munkahelyen történő biometrikus adatkezelésre, a körülményektől függően.

Mindenképp fontos szempont, hogy az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges-e az adatkezelés, továbbá az adatkezelés arányossága fennáll-e, amit a munkáltatónak kell megfelelően bizonyítania és dokumentálnia egy érdekmérlegelési tesztben.

²⁰ <https://www.parlament.hu/irom41/04479/04479.pdf> (letöltve 2024. 11. 14.)

Az érdekmérlegelés alapján csak akkor alkalmazható a jogos érdek jogalap az adatkezelésre, ha az érintettek jogai és szabadságai az adott esetben nem élveznek elsőbbséget, és ennek világos és valós oka megfelelően bemutatásra és dokumentálásra kerül. Az arányosság elvének egyik központi kérdése, hogy van-e alternatívája a biometrikus rendszer alkalmazásának.

Az adatkezelő minden esetben köteles ellenőrizni, hogy egyes alternatív intézkedések lehetnének-e a kitűzött célra tekintettel ugyanolyan hatékonyak, de kisebb beavatkozással járók, és köteles ezeket az alternatívákat választani. Természetesen vannak esetek, amikor a biometrikus rendszerek használata az adatkezelő jogos érdekét szolgálja.

Az ilyen érdeken alapuló adatkezelés azonban csak akkor jogszerű, ha az adatkezelő bizonyítani tudja, hogy az érdeke objektív módon magasabb rendű az érintett adatvédelmi jogainál, melynél ismét az Adatvédelmi Munkacsoport a 6/2014. számú véleményében is felhozott, halálos vírust kezelő laboratórium a példa.

8. Nemzetközi kitekintés

Az ujjlenyomat munkahelyen történő alkalmazásával kapcsolatos Holland Adatvédelmi Hatóság (AP) által hozott döntést mutatok be.

Egy cég alkalmazottainak ujjlenyomatát kellett beolvasniuk a jelenlét és az idő regisztrálása céljából. Az AP egy vizsgálat után arra a következtetésre jutott, hogy a cégnek nem kellett volna az alkalmazottak ujjlenyomatait feldolgoznia. A társaság különleges személyes adatok kezelése esetén nem hivatkozhat kivételre. A céget ezért 725 ezer euróra büntették, azonban ezt később 50 ezer euróra csökkentették, a korona vírus válság okozta gazdasági helyzetre tekintettel. A biometrikus adatok, például az ujjlenyomat speciális személyes adatok. Egy szervezet különleges személyes adatot nem használhat fel, kivéve, ha jogszabály kivételt tartalmaz. Monique Verdier, az AP alelnöke: „A személyes adatok ezen kategóriája fokozottan védett a törvény által. Ha ezek az adatok rossz kezekbe kerülnek, az helyrehozhatatlan károkat okozhat. Ilyen például a zsarolás vagy a

személyazonosság-csalás. Az ujjlenyomat nem cserélhető, mint a jelszó. A hatás jelentős lehet, és egy életre negatív hatással lehet valakire.

A tilalom alól 2 kivétel lehetséges az ujjlenyomatok használatára vonatkozóan:

1. az érintettek kifejezett hozzájárulása;
2. ha biometrikus adatok használata hitelesítéshez vagy biztonsági okokból szükséges

Az AP arra a következtetésre jutott, hogy ez a vállalat nem hivatkozhat a két kivétel közül az elsőre az alkalmazottak ujjlenyomatainak gyűjtése, tárolása és felhasználása során. A munkáltató megkérheti a munkavállalót, hogy adjon ujjlenyomatot például a hozzáférés-szabályozáshoz. Az, hogy a munkáltató köteles-e megadni az ujjlenyomatot, az attól függ, hogy az ujjlenyomat feldolgozása szükséges-e a hitelesítéshez vagy a biztonsághoz.

A munkáltatónak mérlegelnie kell, hogy az épületeket és az információs rendszereket olyan jól kell-e védeni, hogy ezt ne érhesse el másként, mint (csak) biometrikus adatok használatával. Ez az igény gyakran nem lesz indokolt, mert vannak jó alternatívák.

Az adatvédelmi törvény szigorú követelményeket támaszt a kifejezett hozzájárulás kérésére. A hozzájárulásnak egyértelműnek, konkrétan, tájékozottnak és ingyenesnek kell lennie.

Ez a vállalat nem bizonyította, hogy alkalmazottai kifejezett beleegyezést adtak volna. Az alkalmazottak kötelességként élték meg az ujjlenyomat rögzítését is.²¹

9. *Eltérések a büntetőeljárás és a munkajogi adatvédelmi követelmények között*

Ahogy arra már az GDPR és az Info tv. alkalmazásának kérdéskörében már kitértem, a biometrikus adatok kezelésének szempontjából különösen szemléletes a büntetőeljárásban és a munkajogi, illetve tágabb értelemben polgári jogi viszonyokban alkalmazandó eljárási szabályok összehasonlítása.

²¹ <https://autoriteitpersoonsgegevens.nl/actueel/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers> letöltve 2024. 11. 14.: Határozat letöltve: https://autoriteitpersoonsgegevens.nl/uploads/imported/onderzoek_vingerafdrukken_personeel.pdf (letöltés ideje 2024. 11.14.)

A biometrikus adatok sajátos tulajdonsága, úgy mint egyediség, állandóság és a természetes személyhez való erős kapcsolódás, indokolja, hogy a jogalkotó mind az uniós, mind a tagállami szinten a személyes adatok különösen érzékeny kategóriájaként kezeli őket. A biometrikus azonosítók jellemzően olyanok, amelyek alkalmasak egy személy egyértelmű és megbízható azonosítására még akkor is, ha más személyes adatok hiányoznak vagy szándékosan megváltoztatásra kerültek. Ebből fakad és ahogy azt történeti áttekintés alapján láttuk, hogy az ujjlenyomat használat egyik legrégebbi felhasználási területének a bűnüldözés számít.

Az ujjnyomatokra épülő magyar bűnügyi nyilvántartásra több, mint száz éves múltra tekint vissza. A Magyar Igazságügyi Szakértői Kamara honlapján²² fellelhető kamara története szerint 1909-ben jött létre az Országos Bűnügyi Nyilvántartó Hivatal, amelynek keretében működött a Bűnügyi Laboratórium, ahol ujjnyom-, lábnyom-, írás-, lőfegyver-, vérfolt-, textilvizsgálatot, fényképezési tevékenységet végeztek, szakvéleményeket készítettek.

Nyilvánvaló, hogy a biometrikus adatok kezelése – akár hatósági, akár magánjogi kontextusban történik – csak szigorú korlátok között képzelhető el. A büntetőeljárás jellege miatt is szigorúan megköveteli a jogszabályi garanciák érvényesülését.

A bűnügyi nyilvántartás szabályait a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény tartalmazza.

A jogszabály értelmező rendelkezési között találjuk a daktiloszkópiai nyilvántartás defincióját. A jogszabályban külön fejezet rendelkezik a bűnügyi és rendészeti biometrikus adatok, így a daktiloszkópiai adatok nyilvántartásáról, mely a jogszabály indokolás szerint újraszabályozza az ujj- és tenyérynymatokat, valamint DNS-profilokat tartalmazó nyilvántartások rendszerét és adattartalmát.

²² <https://misk.hu/index.php/misk/a-kamara-tortenete> (letöltés ideje 2025. 11.17.)

Mind a daktiloszkópiai mind a DNS-profil nyilvántartások (a továbbiakban együtt: bűnügyi és rendészeti biometrikus nyilvántartás) további egymástól elkülönülő nyilvántartásokra tagozódnak, annak érdekében, hogy a büntetőügyekben rögzített adatok, a 144/2008. (XI.26.) AB határozatnak megfelelő, az adatalanyok eltérő helyzete alapján differenciált kezelése biztosított legyen. Ezen Alkotmánybírósági határozat adatvédelmi szempontból is jelentős, mivel a jogszabály a daktiloszkópiai nyilvántartást három egymástól elkülönülő, a kezelt adatok alanyainak eltérő jogi helyzetét figyelembe vevő részre bontja.

Mindhárom nyilvántartásban fontos érvényesülnie adatvédelmi garanciáknak, azonban közvetlen érintettség szempontjából a büntetőeljárás alá vont személyek ujj- és tenyérnyomatainak nyilvántartásából, valamint a bűncselekmény elkövetése miatt jogerősen elítélt személyek ujj- és tenyérnyomatainak nyilvántartásába kerülésnek van leginkább adatvédelmi jelentősége, mivel ezen biometrikus adatok egyértelműen kapcsolhatók azon személyhez akitől levételre kerültek, ellentétben a bűncselekmény helyszínén és a bűncselekmény elkövetésének nyomait hordozó tárgyon rögzített ujj- és tenyérnyomatokkal. Természetesen ez utóbbi nyilvántartásba kerülés olyan személyt is érinthet, aki az adott bűncselekményben elkövetőként nem érintett, és ez felvethet további adatvédelmi aggályokat, éppen ezért nagy jelentőségű a nyilvántartások ilyen módon történő elválasztása.

A jogszabály egyértelműen meghatározza, hogy mely esetekben kerül sor erre és egyértelműen meghatározza a kezelt adatok körét.²³ és az adatkezelés módját. Nyilvánvalóan ezen esetekben a már tárgyalt munkajogi illetve polgári jogi, azaz GDPR-ban szabályozott hozzájárulás mint jogalap szóba se jön, ezen mintavétel az érintett akarat ellenére is kikényszeríthető²⁴, mint legnyilvánvalóbb különbség, mivel a büntetőeljárásban az állami szervek közhatalmi felhatalmazás alapján járnak el, azzal szemben, hogy a munkahelyi környezetben a cél nem közhatalmi jellegű, és nem is kapcsolódik a társadalom egészének védelméhez, így az érintettek alapjogainak korlátozása jóval szűkebb körben igazolható és nyilvánvalóan kényszer alkalmazása kizárt.

²³ 2009. évi XLVII. tv. 44. § és 48. §

²⁴ 2009. évi XLVII. tv. 95. § (2) bekezdés

Fontos különbség az érintetti jogok és az autonómia szerepe, mivel a GDPR alapján a biometrikus adatok munkahelyi kezelése során az érintett autonómiájának védelme meghatározó. Az érintett hozzájárulása - még ha formálisan megadott is - gyakran nem tekinthető önkéntesnek a munkáltató és munkavállaló között fennálló alá-fölérendeltségi viszony miatt. Ezért a hozzájárulás a gyakorlatban ritkán megfelelő jogalap, és a munkáltatónak más, erősebb indokot kell felmutatnia (pl. jogos érdek vagy jogi kötelezettség), amely körülmény azonban biometrikus adatok esetén a büntetőeljárásban nem áll fenn.

A két jogterület közötti különbség abban is megmutatkozik, hogy a hatósági eljárás szigorúan formalizált, míg a munkahelyi adatkezelés szempontjából a dokumentálás és transzparencia kulcsfontosságú, hiszen ez bizonyítja a jogszerűséget.

A büntetőeljárásban történő adatkezeléssel szemben a munkáltató adatkezelési kötelezettségei ugyan szintén kötelezőek, azonban jellegüknél fogva azok alapja sokkal inkább a megelőző, kockázatalapú megközelítés. A GDPR szerinti garanciák tehát nemcsak eljárási szabályok, hanem olyan általános elvek és technikai-szervezési követelmények, amelyek célja a visszaélések megelőzése és a munkavállalók alapjogainak megóvása.

10. Összegzés

Jelen tanulmányban felvázoltak alapján megállapítható, hogy általánosságban a biometrikus rendszerek alkalmazása nem elengedhetetlen és nem a legkíméletesebb eszköz a munkavállalók ellenőrzésénél. Így például az ujjlenyomatos munkaidő-nyilvántartással kapcsolatban megállapítható, hogy a munkavállalók ellenőrzését, mint célt más, a magánszférát kímélőbb módszerekkel is el lehet érni, ezért ebből a célból nem lehet biometrikus rendszert bevezetni. Alkalmazásuk jogszerűségéhez szigorú adatvédelmi és munkajogi szabályoknak kell megfelelni.

A külföldi példa alapján is látható, hogy a munkahelyen alkalmazni kívánt biometrikus azonosítók vonatkozásában nemzetközi viszonylatban is a hazai szabályozással és állásponttal megegyező szigorú követelmények érvényesülnek.

Az ujjlenyomat olvasó technológia olcsósága és könnyű hozzáférhetősége sok - különösen kevés munkavállalót foglalkoztató - munkáltatót elgondolkoztat, hogy ilyen technológiával oldják meg akár a munkaidő nyilvántartást, de mint a dolgozatomban kifejtettek alapján látszik, az ezzel kapcsolatos adatvédelmi követelmények meghaladják a vele elérhető előnyöket.

Használatának adatvédelmi aggályain és előírásain túl nem szabad elfelejtkezni az emberi oldalról sem, ugyanis bár elméletileg nem túlzottan beavatkozó jellegű módszerről van szó, mégis ezt a benyomást keltheti, mivel a bűnüldözés terén való elterjedt használata miatt az a kedvezőtlen kép alakulhat ki az egyénben, hogy gyanúsítottként kezelik.

A büntetőeljárásban érvényesülő adatvédelmi követelményekkel való összevetése rávilágít arra, hogy bár a két rendszer eltérő funkciót lát el, mindkettő szigorúan szabályozza a biometrikus adatok kezelését. A büntetőeljárási keretek a közérdek érvényesítése érdekében korlátozzák az érintett jogait, míg a GDPR-nak való megfelelés a magánszféra védelmét helyezi előtérbe. Ebből következően a munkahelyi biometrikus adatkezelés - amely nem rendelkezik a büntetőeljárási adatkezelés törvényi felhatalmazásával - csak rendkívül szűk körben tekinthető jogszerűnek. A büntetőeljárási gyakorlat így indirekt módon igazolja a biometrikus adatok érzékenységet és a rájuk vonatkozó adatvédelmi garanciák szükségességét.

A biometrikus adatok büntetőeljárási kezelésének jogi keretei egyúttal megmutatják, hogy a jogalkotó mit tekint e különleges személyes adatok lényegi sajátosságának. A büntető igazságszolgáltatás területén fennálló szigorú garanciarendszer evidencia arra, hogy a biometrikus adatok olyan érzékeny információk, amelyekkel kapcsolatban az állami szervek is csak korlátozottan, jól körülhatárolt cél érdekében és kizárólag törvényi felhatalmazás alapján járhatnak el. Ez azért különösen releváns a munkahelyi adatkezelések vizsgálatakor, mert rávilágít: ha a biometrikus adatokkal való eljárás a büntetőeljárásban is fokozott jogi kontroll alatt áll, akkor a munkáltatók adatkezelési tevékenysége - amely nem közhatalmi jellegű - csak még szűkebb és szigorúbb feltételek mellett lehet jogszerű.

A biometrikus adatok büntetőeljárásban való kezelésének szabályai továbbá rámutatnak a célhoz kötöttség és az arányosság elvének kiemelkedő szerepére. A bűnüldöző szervek kizárólag

meghatározott célok - például személyazonosítás, körözött személy azonosítása vagy bűncselekmény felderítése - érdekében használhatják fel az ilyen jellegű adatokat. A célhoz kötöttség elvének ilyen fokú érvényesülése pedig közvetett módon megerősíti azt a munkajogi- és adatvédelmi gyakorlatot, amely kimondja: a munkáltató csak akkor alkalmazhat biometrikus azonosítást, ha az feltétlenül szükséges, és nincs más, kevésbé invazív alternatíva ugyanazon cél elérésére.

Természetesen a folyamatosan fejlődő technológia és ebből adódó jogi feladatok folyamatos fejlődésre készítetik az adatvédelmi szabályok megalkotóit és azok alkalmazóit.

Alkalmazott jogszabályok és irodalom, honlapok

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- 2012. évi I. törvény a munka törvénykönyvéről
- a bünygyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bünygyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
- A 29. cikk szerinti adatvédelmi munkacsoport 06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról (WP 217)
- A 29. cikk szerinti adatvédelmi munkacsoport 3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről (WP 193)
- 4/2007. sz. vélemény (WP136)
- NAIH/2019/1074 számú tájékoztató
- A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről Budapest, 2016. október 28.
- KOVÁCS T. - MILÁK I. - OTTI Cs.: A biztonságtudomány biometria i aspektusai
<http://www.pecshor.hu/periodika/XIII/kovacsti.pdf>, (letöltve: 2024.11.14.)
- <http://fingerprints.handresearch.com/dermatoglyphics/fingerprints-world-map-whorls-loops-arches.htm> Martijn van Mensvoort MAY 11, 2011 [LAST UPDATES: MARCH, 2015]
letöltve 2024. 11. 14.
- <https://autoriteitpersoonsgegevens.nl/actueel/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers>
- <https://www.parlament.hu/irom41/04479/04479.pdf>