



Ügyszám: NAIH-2269-4/2014/V.

Dr. Nagy Zoltán Zsolt részére
igazgató

Semmelweis Egyetem ÁOK Szemészetli Klinika

Budapest
Mária utca 39.
1085

Tisztelt Igazgató Úr!

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) megkapta válaszlevelét, amelyben a Semmelweis Egyetem ÁOK Szemészetli Klinikáján (a továbbiakban: Klinika) bevezetett ujjnyomat-azonosítás alapján működő biometrikus rendszerrel kapcsolatban az alábbi tájékoztatást nyújtotta:

Elmondása szerint a bejelentő által kifogásolt biometrikus rendszer működése során az érintett ujjnyomatából képzett kódot tárolja el, és veti össze a belépésnél levett ujjnyomatból képzett kóddal. A rendszer jelenleg még tesztüzem módban működik. Annak bevezetésére amiatt volt szükséges, mert a jelenleg használt mágneskártyás beléptetés visszaélésekre adott lehetőséget. Azt a munkavállalók több esetben is kijátszották. Álláspontja szerint a biometrikus rendszer működtetése során végzett adatkezelés jogalapját a Munka Törvénykönyvéről szóló 2012. évi I. törvény jelenti. Válaszleveléhez csatolta továbbá a munkavállalók részére adott tájékoztató másolatát is.

Az ügyben a Hatóság állásfoglalása a következő:

1. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 3. § 2. pontja értelmében személyes adat az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. Érintett bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy [Infotv. 3. § 1. pont].

1.1. A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv (a továbbiakban: Adatvédelmi Irányelv) 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (a továbbiakban: Munkacsoport) által elfogadott, a biometrikus technológiák fejlődéséről szóló 3/2012. számú vélemény (WP)¹ szerint biometrikus adat a biológiai jellegzetességek, pszichológiai sajátosságok, életvitel vagy olyan ismétlődő tevékenységek, amelyek során e jellegzetességek, tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is.

¹ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf#h2-2.

A fenti meghatározás alapján egy természetes személy ujjnyomata biometrikus adatnak minősül, amely – tekintettel arra, hogy az az érintett fiziológiai azonosságára jellemző ismeret – személyes adat is egyben.

A biometrikus rendszerek alapvetően két eltérő módszer, következésképpen két eltérő adatkör alapján működhetnek. A hagyományos biometrikus rendszerek a működésük során az érintett biometrikus adatról készített felvételt hasonlítják össze az ugyanarról az adatról korábban rögzített és eltárolt felvétellel. Ebben az esetben a technológia minden esetben személyes adatokat dolgoz fel.

1.2. A fejlettebb biometrikus rendszerek ugyanakkor a nyers formában lévő biometrikus adatból kinyert kulcsfontosságú jellemzők alapján ún. biometrikus sablonokat képeznek. Ebbe a körbe tartoznak például a különböző logikai művelettel létrehozott digitális adatcsomagok. A biometrikus sablon képzése egyirányú folyamat, amely lehetetlenné teszi a biometrikus adatok ismételt előállítását vagy visszafejtését.

Az ilyen biometrikus rendszerek kétféle biometrikus sablon alapján működnek: az egyik a letárolt formában lévő, a másik pedig a rendszer működése során keletkezett sablon. A rendszer mindig utóbbit hasonlítja az előbbihez. A két sablon teljes mértékig megegyezhet, vagy – egyes esetekben – előre meghatározott százalékos mértékig eltérhet egymástól. A Klinikán bevezetett ujjnyomat-azonosítás alapján működő biometrikus rendszer az utóbbi kategóriába esik.

Biometrikus sablon – szemben a biometrikus adattal – csak akkor nem minősül személyes adatnak, ha azok tárolása oly módon történik, hogy az érintett azonosítására semmilyen ésszerű eszköz nem áll az adatkezelő vagy harmadik személy rendelkezésére. Amennyiben tehát a letárolt sablont megszemélyesítik, ahhoz további adatokat (a továbbiakban: azonosító adat) rendelkeznek, az adatcsomag személyes adatnak fog minősülni.

Végezetül a Hatóság hangsúlyozni kívánja azt, hogy noha a biometrikus adat és a biometrikus sablon fogalma nem fedi le egymást, adatvédelmi szempontból a megítélésük egy tekintet alá esik. A biometrikus információ feldolgozása ugyanis elengedhetetlenül szükséges a sablon képzéséhez. Ily módon mindkettő kezelése esetén felmerül az érintett személy magánszférájának súlyos érintettsége: a biometrikus adat, illetve az abból képzett bármely számsor minden esetben az érintettől elválaszthatatlan információ lesz, hiszen annak feldolgozásához minden egyes esetben szükséges az érintett fizikai jelenléte és személyes adatának szolgáltatása. A biometrikus rendszer ezáltal pedig a mindig hatást gyakorol az érintett privát szférájára. Ezt a tényt a biometrikus rendszereket használó adatkezelőknek minden esetben figyelembe kell venniük.

1.3. Nem kizárt az sem, hogy a biometrikus rendszer üzemeltetése során további, az érintettre vonatkozó adatok is keletkezhetnek. Ilyen lehet például egy adott területre való belépés, vagy az érintett személy azonosítása helyének és idejének időpontja. Az Infotv. alapján ezek az információk is személyes adatnak minősülnek.

2. Az Infotv. 3. § 10. pontja értelmében adatkezelés *„az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyémnyomat, DNS-minta, írszék) rögzítése”*.

A Klinikán bevezetett ujjnyomat-azonosítás alapján működő biometrikus rendszer üzemeltetésével kapcsolatban három fő adatkezelési művelet különböztethető meg. A „biometrikus adatok felvétele” mindazokat a folyamatokat magában foglalja, amelyeket annak érdekében végeznek egy biometrikus rendszer működtetése során, hogy egy biometrikus forrásból biometrikus adatot nyerjenek ki, abból

letárolandó sablont képezzenek, és ezt az adatot hozzákapcsolják az érintetthez. A „biometrikus adat tárolása” alatt a letárolt sablon és a hozzárendelt egyéb személyes adatok megőrzése értendő egy, a leolvasók által hozzáférhető központi adatbázisban. A „biometrikus adatok párosítása” pedig a letárolt sablon összehasonlítása a biometrikus rendszer működése során keletkezett biometrikus sablonnal.

3. Az Infotv. 5. § (1) bekezdése kimondja, hogy személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy ha az törvény azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés).

3.1. Az Infotv. 3. § 7. pontja szerint a hozzájárulás az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. E meghatározásból következően a hozzájárulás érvényességének négy alapvető feltétele létezik: az érintettnek cselekvőképessége, megfelelő és előzetes tájékoztatás, kifejezettség, valamint önkéntesség.

Az önkéntesség követelménye azt jelenti, hogy a hozzájárulást mindenfajta külső befolyástól mentesnek kell megadni. Megkérdőjelezhető az önkéntesség például akkor, ha az adatszolgáltatás megtagadása esetén az érintettet hátrányok érhetik. A foglalkoztatás kontextusában így nehézségek merülhetnek fel az érintett hozzájárulásának önkéntes voltával kapcsolatban, hiszen a munkáltató és az alkalmazott között alá-főlérendeltségi viszony van. A hierarchikus függés e helyzeteiben a munkavállaló adatkezeléssel kapcsolatos elutasítása vagy fenntartása anyagi vagy nem anyagi természetű hátrányt okozhat neki, ami teljes mértékben ellentétes a személyes adatok védelmére vonatkozó európai jogalkotás szövegével és szellemével. A hozzájárulást ezért ebben a tekintetben nem lehet az adatkezelés megfelelő jogalapja.

3.2. Az Infotv. 5. § (1) bekezdés b) pontja szerinti kötelező adatkezelést elrendelő jogszabály lehet mind az országgyűlés által megalkotott törvény, mind pedig helyi önkormányzat rendelete. A törvénnyel szemben az adatvédelemmel kapcsolatban támasztott tartalmi garanciákat az Infotv. 5. § (3) bekezdése tartalmazza: *„Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.”*

További vizsgálandó szempont az, hogy a Hatóság – figyelemmel a korábbi adatvédelmi biztosi gyakorlatra – nem csak azt tekinteli kötelező adatkezelésnek, amikor a jogszabály kifejezetten „elrendeli” az adatkezelést, hanem akkor is, ha pusztán „lehetővé teszi” vagy ha az adatok kezelése szükségszerű velejárója egy bizonyos tevékenységnek. Ebbe a körbe tartozik például a munkáltató ellenőrzési jogosultsága a munkavégzés tekintetében. Ilyenkor azonban az adatkezelést elrendelő jogszabálynak külön garanciákat kell tartalmaznia az érintettek magánélet tiszteltben tartásához, illetőleg személyes adatok védelméhez fűződő jogainak maximális érvényesülése érdekében.

3.3. Az Mt. 134. § (1) bekezdése értelmében a munkáltató köteles nyilvántartani a rendes és a rendkívüli munkaidő, a készenlét és a szabadság tartamát. A nyilvántartásból naprakészen megállapíthatónak kell lennie a teljesített rendes és rendkívüli munkaidő, valamint a készenlét kezdő és befejező időpontjának is [Mt. 134. § (2) bekezdés]. A Mt. 134. § (3) bekezdésében viszont külön is hangsúlyozza, hogy a munkaidő nyilvántartás *„az írásban közölt munkaidő-beosztás hónap végén történő igazolásával és a változás naprakész feltüntetésével is vezethető”*.

Az Mt. idézett rendelkezéseiből következően a munkáltatónak nemcsak joga, de kötelezettsége is egyben az, hogy a munkavállalók munkaidejének ellenőrzése és nyilvántartása. Ebből következően – összhangban az Infotv. 5. § (1) bekezdés b) pontjával kapcsolatban kifejtettekkel – megállapítható, hogy a Klinika jogosult az

Mt.-ből eredő kötelezettségének teljesítése során az érintett munkavállalók személyes adatait kezelni. Ez azonban nem történhet korlátlanul, figyelembe kell ugyanis venni a munkavállalók személyiségi jogait védő rendelkezéseket is.

A munkavállaló személyes adatainak kezelésére vonatkozó alapvető követelményeket a Munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 10. § (1) bekezdése határozza meg. Eszerint *„[a] munkavállalótól csak olyan nyilatkozat megtétele vagy adat közzétevése kérhető, amely személyhez fűződő jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.”*

Az Mt. értelmében a munkáltatónak két konjunktív feltétel teljesülését kell az adatkezelés előtt megvizsgálnia ahhoz, hogy a munkavállalók adatait kezelhesse. E feltételek közül az első és egyben legfontosabb az, hogy az adatok felvétele, rögzítése és felhasználása nem sértheti a munkavállalók személyhez fűződő jogait. Amennyiben ugyanis a munkáltató döntés ennek nem felel meg, a második kritérium, vagyis a munkaviszony létesítésével, teljesítésével vagy megszüntetésével való összefüggés vizsgálata irrelevánssá válik.

A személyhez fűződő jogok esetleges sérelmének vizsgálata szempontjából további lényeges rendelkezés az Mt. 9. § (1) bekezdése, amely a törvény fent idézett előírásával korrelatív kapcsolatban áll. Az Mt. 9. § (1) bekezdése értelmében a törvény hatálya alá tartozók személyhez fűződő jogait tiszteletben kell tartani. A munkavállaló személyhez fűződő joga akkor korlátozható, ha a korlátozás a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges és a cél elérésével arányos. A személyhez fűződő jog korlátozásának módjáról, feltételeiről és várható tartamáról a munkavállalót előzetesen tájékoztatni kell [Mt. 9. § (2) bekezdés].

A törvényhez fűzött indokolás szerint az Mt. 9. § (2) bekezdése általánosságban fogalmazza meg a munkavállaló személyhez fűződő jogai korlátozásának alapvető elveit és egyben rögzíti annak határait. A törvény a személyhez fűződő jogok védelme érdekében a munkáltató eljárásával összefüggésben két szigorú feltételt állapít meg. Ennek az eljárásnak kizárólag és közvetlenül a munkáltató rendeltetésszerű működésével kell összefüggésben lennie, ezen a körön nem terjeszkedhet túl.

A rendeltetésszerű működés ebben a kontextusban is szűken értelmezendő. A munkáltató az eljárás bevezetéséről csak abban az esetben dönthet, amennyiben az feltétlenül, azaz objektíve szükséges. Ebből a szempontból lényeges, hogy a munkaidő nyilvántartása mint munkáltatói kötelezettség teljesítése – általánosságban – megfelel az objektív szükségesség kritériumának.

Az objektív szükségesség követelményén túl az Mt. azonban megfogalmazza az arányosság kritériumát is. Ebben a vonatkozásban a Hatóság irányadónak tekinteti a Munkacsoport korábban idézett véleményét, amely szerint a biometrikus adatok csak akkor kezelhetők, ha megfelelőek, relevánsak és nem túlzott mértékűek, ezért a kezelt adatoknak meg kell felelniük a szükségesség és az arányosság követelményének. Mértegelni kell továbbá, hogy a biometrikus rendszer üzemeltetése által elért kívánt cél megvalósítható lenne-e egyéb, a magánszférát kevésbé érintő módon.

A biometrikus rendszer arányosságának elemzésekor az alábbi szempontokat kell megfontolni:

- A rendszer működtetése szükséges-e a meghatározott cél eléréséhez (szükségesség). Azaz a rendszer használata elengedhetetlen-e az adott igény kielégítéséhez, vagy csupán annak kényelmes és költséghatékony módja.
- A rendszer működtetése mennyire lesz hatékony az adott cél elérése érdekében (hatékonyság).
- A magánszférának a rendszer működtetéséből eredő korlátozása vajon arányban áll-e a várható előnyökkel (arányosság). Amennyiben viszonylag kisebb az előny, például a kényelem növekszik a rendszer működtetése által vagy az csak egy minimális költségmegtakarítást eredményez, akkor a magánszféra korlátozása nem arányos az elérendő célokkal.

- A kitűzött célt vajon el lehet-e érni a magánéletet kevésbé korlátozó módon (**megfelelő alternatívák hiánya**). Amennyiben egyes alternatív intézkedések ugyanolyan hatékonyak lennének a kitűzött célra tekintettel, a rendszer üzemeltetője köteles az alternatívák közül választani.

A fenti követelményekkel kapcsolatban a Hatóság egyrészt hangsúlyozza, hogy – mivel jelentős mértékben érinti az érintettek magánéletét – a biometrikus rendszer működtetése csak akkor minősül jogszerűnek, ha objektív és dokumentált körülmények alapján bizonyított, hogy ténylegesen jelentős kockázat áll fenn a védett terület vonatkozásában. Rizikót jelentő tényezők elsősorban a következők: a minősített adatok, illetve különösen jelentős értékű ingóság vagy pénz védelme, lőfegyver, lőszer, robbanóanyag, mérgező, illetőleg veszélyes vegyi, biológiai és nukleáris anyagok őrzése. A munkaidő nyilvántartás vezetése tehát nem minősül olyan célnak, amelynek elérése érdekében a biometrikus rendszer elengedhetetlenül szükséges lenne.

Másrészt a megfelelő alternatívák hiányának követelménye csak abban az esetben teljesül, ha valóban nem létezik más olyan módszer, amely kevésbé valószínű megbeavatkozást az érintettek magánéletébe. Mivel azonban maga az Mt. biztosít olyan lehetőséget a 134. § (3) bekezdésében, amely a biometrikus rendszer megfelelő alternatívája, ezért annak működtetése nem felel meg az arányosság követelményének sem.

4. A fentiekből következően a Klinikán bevezetett ujjnyomat-azonosítás alapján működő biometrikus rendszer működtetése ellentétes az Mt. 9-10. §-ában foglalt követelményekkel, ezáltal pedig súlyosan sérti az érintettek személyes adatok védelméhez fűződő jogát.

A Hatóság ezért az Infotv. 56. § (1) bekezdése alapján felszólítja a Klinikát arra, hogy haladéktalanul szüntesse meg a biometrikus rendszer keretében végzett adatkezelést. Kérem továbbá, hogy a megtett intézkedéseiről a jelen állásfoglalás kézhezvételét követő 30 napon belül írásban tájékoztassa a Hatóságot.

Budapest, 2014. november. 14.

Üdvözlettel:

Postai úti levél.
2014. 11. 14. LJ


Dr. Péterfalvi Attila
elnök
c. egyetemi tanár