Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH/2015/4674/2/J
Hiv. szám: IV/6-5/2015.
Előadó: dr. Bíró János, dr. Búzás Péter

Magyarország Alkotmánybírósága

Budapest

Tisztelt Alkotmánybíró Asszony!

Megtisztelő felkérésének eleget téve az alábbiakban közlöm a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban Hatóság) válaszát a hivatkozott számú levelében feltett kérdésekre.

1. Megerősíti-e azt a korábban adatvédelmi biztosként – a 2001. évi beszámolójában – kifejtett álláspontját, hogy az adat akkor is megőrzi személyes jellegét, ha az adatkezelő informatikai rendszere nem alkalmas azok értelmezésére?

A kérdés megválaszolásának kiindulópontja a személyes adat törvényi meghatározása, amelyet 2001-ben a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban Avtv.) 2. § 1. pontja állapított meg („*személyes adat: a meghatározott természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható*„). Noha 2012. január 1. óta a személyes adatok védelmének alapvető szabályait már nem az Avtv., hanem az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban Infotv.) állapítja meg, a személyes adatra vonatkozó értelmező rendelkezés, az Infotv. 3. § 2. pontja a korábbiakhoz képest szempontunkból lényegében nem változott („*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*„)

Az Infotv. fogalom-meghatározásából következően a személyes adatoknak két általános csoportja

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.
Tel.: +36 1 391-1400
Fax: +36 1 391-1410
ugyfelszolgalat@naih.hu
www.naih.hu

különböztethető meg. Egyrészt személyes adatnak minősül az érintettel kapcsolatba hozható bármely adat. Ebbe a körbe tartozik különösen az adatalany neve, azonosító jele, egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret, illetőleg a képmása, hangja és az adatalany azonosítására alkalmas fizikai jellemzők (pl. ujjnyomat, DNS minta). Másrészt az adatból levonható, az érintettre vonatkozó következtetés is személyes adat. Ezen információkat azért vonja a szabályozás a védelem körébe, mert számos adatkezelésnek éppen az a célja, hogy a felvett információkból az érintettre vonatkozó következtetéseket vonjon le, amelyek az adatalannyal kapcsolatos döntések alapját képezik (pl. hitelképesség, támogatásokra és kedvezményekre való jogosultság, vagy adott munkakör betöltésére való alkalmasság).

Az adatkezelés szempontjából az „érintett" bármely olyan meghatározott természetes személy lehet, aki személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható (Infotv. 3. § 1. pont). Így érintettnek tekinthető egyrészt az azonosított természetes személy (például név és képmás alapján azonosított személy), másrészt a közvetlenül azonosítható természetes személy (például az ügyfélkód alapján az adatkezelő ügyintézője azonosítani tudja az ügyfelet), végezetül pedig a közvetetten azonosítható személy (bizonyos információk összegsége alapján meghatározható a személy kiléte).

Egy információ személyes adat mivoltának vizsgálata során figyelmet kell szentelni továbbá az „azonosított" és „azonosítható" kifejezéseknek is. Az egyént akkor tekintjük általánosságban azonosítottnak, ha a természetes személyek adott csoportján belül elkülönül a csoport többi tagjától. Az azonosíthatóság pedig az azonosítás megtételének lehetőségét jelenti. Az azonosíthatóság ezért egy küszöbfeltétel, amely meghatározza, hogy az információ személyes adatnak minősül-e. A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv (a továbbiakban: Irányelv) (26) preambulum bekezdése ezzel kapcsolatban kimondja, hogy „annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására". A hazai adatvédelmi gyakorlat szempontjából kiemelendő továbbá, hogy az azonosíthatóság fogalmát kiterjesztően értelmezi, azaz az információ személyes adat jellege nem függ az azt megismerő szubjektív adattartalmától, így irreleváns az, hogy az adatkezelő megfelelő egyéb ismeretek birtokában saját maga képes-e az érintett azonosítására.

Különbség van az érintett azonosítása/azonosíthatósága és személyazonossága között. Előbbi esetben a kezelt adatok módon lehetővé teszik az érintett szeparálását környezetétől vagy az ott lévő harmadik személyektől. Az azonosítás/azonosíthatóság arra a kérdésre ad választ tehát, hogy a kezelt információk mely személyhez tartoznak a csoporton belül. Ezzel szemben a személyazonosság annak megállapítását teszi lehetővé, hogy pontosan ki is az adott egyén. Az adatkezelő ezáltal felismeri az érintettet. Az érintett identitásának megállapításához jellemzően jogszabályokban meghatározott különféle azonosítókat alkalmaznak az adatkezelők. Az említett információk legjellemzőbb és Magyarországon leggyakrabban használt kategóriáját a természetes személyazonosító adatok jelentik. A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 4. § (4) bekezdése értelmében a polgárok természetes személyazonosító adatai a következők: családi és utónév, születési családi és utónév; születési hely; születési idő és anyja születési családi és utóneve.

Az érintett azonosítása/azonosíthatósága és személyazonossága közötti különbség abból a szempontból releváns, hogy a magyar jogi gondolkodásban és a hétköznapi gyakorlatban is az gyökeresedett meg, hogy csak abban az esetben beszélhetünk személyes adatokról, amennyiben azáltal az érintett abszolút módon – minimálisan névvel, esetleg még egy vagy több további információ révén – azonosított. Ez azonban rendkívüli módon leszűkítené a személyes adat

fogalmát, ezáltal pedig az egyén magánéletének háborítatlanságát biztosító adatvédelmi garanciák alkalmazásának körét. Ahogy arra az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport a személyes adat fogalmáról szóló 4/2007. szánú véleményében (WP136) rámutatott – az érintett azonosíthatóságát nemcsak egyedi, csak az adott személyhez köthető információk tehetik lehetővé. Bizonyos adatok egyedi kombinációja révén ugyanis az adatkezelő képes közvetve azonosítani az érintett személyt. „Azokban az esetekben, ahol a hozzáférhető azonosítók kiterjedése első látásra nem teszi senki számára lehetővé az adott személy kiválasztását, attól még e személy 'azonosítható' lehet, mivel az említett információ más információkkal összekapcsolva (ez utóbbi akár megvan az adatkezelőnél, akár nincs) az egyént másoktól megkülönböztethetővé teszi."

A fentiek értelmében az Infotv. idézett 3. § 1. pontja szerint az adat személyes jellegét az adja, hogy az az érintettel kapcsolatba hozható, illetve rá vonatkozó következtetést tartalmaz. Ami az adat és az érintett közötti kapcsolatot illeti, kiemelendő, hogy az idézett értelmező rendelkezés nem kívánja meg azt, hogy az érintett és az adat közötti kapcsolat adott időpontban ténylegesen fennálljon, hanem elégséges az érintett és az adat közötti kapcsolat helyreállításának lehetősége is. Az értelmező rendelkezés a kapcsolat helyreállításának lehetőségét nem szűkíti le valamely, e szempontból kitüntetett helyzetben lévő adatkezelőre, például arra az adatkezelőre, amely éppen az adat birtokában van. Ebből következően az adat személyes jellege nem szűnik meg pusztán attól, hogy az az adatkezelő, melynek birtokában van, éppen nem képes az adat értelmezésére (például azért, mert az adatokat zárolták vagy kódolták, vagy az adatkezelő informatikai rendszere éppen nem működik megfelelően). Ha az adott adatkezelő nem képes az adatot értelmezni, akkor az idézett értelmező rendelkezésben foglaltak közül az érintettre vonatkozó következtetés levonására ugyan nem képes, de az adat és az érintett közötti kapcsolat változatlanul fennmarad, és ha az adott adatkezelő később ismét képessé válik az adat értelmezésére, vagy olyan másik adatkezelőnek továbbítja az adatot, amelynél az adat értelmezése nem ütközik akadályba, akkor az adatok megszemélyesítése, az érintettel összefüggésben történő felhasználása, az érintettre vonatkozó következtetés levonása lehetségessé válik.

Az Infotv. 4. § (3) bekezdése szerint a személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek. A személyes adat törvényi értelmező rendelkezésével, valamint a fentiekben kifejtettekkel összhangban úgy értelmezzük az Infotv. 4. § (3) bekezdésében foglaltakat, hogy az adat személyes jellegének megítélésekor nem azt kell vizsgálni, hogy az adat és az adatalany közötti kapcsolat valamely konkrét adatkezelő számára az adott időpontban helyreállítható-e, hanem azt, hogy a lehetséges adatkezelők bármelyike számára lehetséges-e e kapcsolat helyreállítása.

Az előbbiektől meg kell különböztetni azt az esetet, ha az adat véglegesen, bármely lehetséges adatkezelő által értelmezhetetlenné válik, vagy az adat és az érintett közötti kapcsolat bármely lehetséges adatkezelő számára helyreállíthatatlanul megszűnik. Ebben az esetben az adat személyes jellege kétségtelenül megszűnik. Ez történik az adat törlése vagy megsemmisítése, illetve megsemmisülése esetén.

Azt, hogy az adat értelmezhetetlenné válása csak ideiglenes-e vagy végleges, továbbá az adat csak adott adatkezelő számára válik értelmezhetetlenné vagy valamennyi lehetséges adatkezelő

számára, továbbá, hogy megszakadt-e, és véglegesen szakadt-e meg az adat és az érintett közötti kapcsolat, azt mindig konkrét a adatkezelést és annak körülményeit gondosan megvizsgálva lehet megállapítani.

Megjegyezzük, hogy a fentiektől eltérő értelmezés – nevezetesen az, hogy az adat személyes jellege megszűnik azáltal, ha az adatot birtokló adatkezelő nem képes értelmezni azt – nem lenne összhangban a személyes adatok védelmének követelményeivel, ugyanis olyan adatok esetében is megszüntetné az adatkezelő jogi felelősségét, amelyek esetleg csak átmenetileg értelmezhetetlenek az adott adatkezelő számára, illetve más adatkezelők által minden további nélkül felhasználhatók az érintettel összefüggésben.

2. Jelenlegi gyakorlata szerint a biometrikus adatból képzett kódot (a biometrikus sablont) személyes adatnak tekinti-e?

A válasz egyértelműen igen. A biometrikus sablont az érintett személyes adatából vagy adataiból hozzák létre. Jóllehet a biometrikus sablon nem azonos azzal a személyes adattal vagy azokkal a személyes adatokkal, amelyekből létrehozták, ám az érintettel kapcsolatba hozható és rá vonatkozó következtetés levonására alkalmas. Továbbmenve, a biometrikus sablon rendszerint személyazonosító adat, tehát kétségtelenül személyes adat. Hatóságunk ugyanakkor nem tesz különbséget a biometrikus adatok, illetőleg a biometrikus sablonok között az alkalmazandó adatvédelmi előírások és garanciák tekintetében. A vonatkozó gyakorlat a biometrikus sablonok használata esetén is a biometrikus adatok kezelésével összefüggő előírások betartását követeli meg.

3. Mennyiben hat ki a biometrikus sablon jogi jellegének megítélésére, hogy visszafejthetetlen kódoláson alapul?

A biometrikus sablon létrehozásakor az érintett bizonyos személyes adatát vagy adatait feldolgozzák (a művelet számításigénye miatt rendszerint gépi úton), kiemelve annak későbbi automatizált felhasználásra, így különösen automatizált keresésre, összehasonlításra, kiválogatásra alkalmas, mérhető jellegzetességeit. A biometrikus sablon létrehozása során az e szempontokból lényegtelen információk elvesznek, ezért a biometrikus sablonból a kiinduló adattartalom teljessége nem rekonstruálható. Ilyen értelemben a biometrikus sablon létrehozása eleve egyirányú kódolással jár. Például egy arckép biometrikus sablonjának létrehozásakor az alkalmazott eljárás kiemel bizonyos jellemzőket és arányokat, mint például a pupillák közötti távolság és egyéb egyéb mérhető jellemzők, de az például nem kerül bele a biometrikus sablonba, hogy a feldolgozott arcképen éppen kócos vagy jól fésült volt-e az érintett haja, ezért a biometrikus sablonból a felhasznált arckép nem állítható helyre.

A biometrikus sablon nem azonos a kiindulási adattal és nem azonosak a kétféle adat felhasználási lehetőségei. Az előbbi példánál maradva az arckép csatolható egy álláskereső pályázathoz, azonban az abból képzett biometrikus sablont nem lenne érdemes ilyen célra felhasználni. Ugyanakkor az arckép biometrikus feldolgozás nélkül kevéssé alkalmas automatizált személyazonosság ellenőrzésre, ám a bioemtrikus sablon annál inkább. Ez azonban nem változtat azon a megállapításon, hogy a biometrikus sablon is személyes adat.

A biometrikus sablon és annak visszafejthetetlen kódolása egy másik szempontból is vizsgálandó:

lehetséges, hogy az adatkezelő a biometrikus sablont további, egyirányú leképezést megvalósító eljárással – például valamelyik úgynevezett hash algoritmus alkalmazásával – átalakítja. Ennek célja például az adat felhasználhatóságának valamilyen korlátozása lehet azért, hogy jobban megfeleljen a személyes adat célhoz kötött kezelésére, vagy az osztott információs rendszerekre vonatkozó adatvédelmi követelményeknek.

- Ha például a biometrikus sablont olyan egyirányú kódolásnak vetik alá, amely kizárja a biometrikus sablonban rögzített adatok – az előbbi példánál maradva például a pupillatávolság – kinyerését, akkor az egyirányú leképezéssel átalakított biometrikus sablon többé nem lesz alkalmas a sablonban rögzített személyes adatok alapján történő leválogatásra, összehasonlításra. Az előbbi példánál maradva: az egyirányú kódolással átalakított biometrikus sablonokat tartalmazó adatbázisból már nem válogathatók le azon személyek adatai, akik éppen a megadott pupillatávolsággal rendelkeznek. Ugyanakkor az ilyen adatbázis továbbra is alkalmas lesz a referencia adatforrásként való felhasználásra személyazonosítás vagy személyazonosság ellenőrzése során. (A személyazonosítás ilyenkor úgy történik, hogy az azonosítandó személyről felvett adatok alapján elkészítik az érintett biometrikus sablonját, majd végrehajtják rajta ugyanazt az egyirányú leképezést megvalósító átalakítást, amit a referencia adatbázis biometrikus sablonjainál is alkalmaztak. Ezek után ezt az adatot összehasonlítják a referencia adatbázisban tárolt, ismert személyazonosságú személyekre vonatkozó, egyirányú átalakításon átesett biometrikus sablonadatokkal. Adategyezőség esetén megtörtént az érintett azonosítása a referencia adatbázisban tárolt adatokkal.)

- A biometrikus sablon utólagos egyirányú, visszafejthetetlen kódolásának másik alkalmazási területe lehet például az érintettre vonatkozó, különféle adatkezelők birtokában lévő adatok összekapcsolhatóságának korlátozása az osztott információs rendszerekre vonatkozó adatvédelmi követelmény érvényesítése céljából.

  Ebben az esetben nem a biometrikus sablon, hanem az abból egyirányú leképezéssel kódolt adat használható egyedi azonosítóként az adatkezelésekben. Egy biometrikus sablonadatból különböző eljárásokkal több kódolt azonosító hozható létre, melyekből a biometrikus sablon nem állítható helyre, továbbá egyik kódolt azonosítóból matematikai módszerrel nem lehet megállapítani, hogy adott kódolt azonosítóhoz mely további kódolt azonosítók tartoznak. Ezért a különböző kódolt azonosítók továbbra is az érintetthez kapcsolhatók, de a különböző kódolt azonosítókat használó adott adatkezelések összekapcsolása e kódolt azonosítók révén nem lehetséges.

A fentiek értelmében az, hogy a biometrikus sablon visszafejthetetlen kódoláson alapul, önmagában nem garancia arra, hogy az adatkezelés megfelel az adatvédelmi követelményeknek. Csak konkrét biometrikus sablon kódolási eljárásra vonatkozóan és ezzel összefüggésben a kód felhasználási körülményeinek ismeretében lehet megalapozott megállapítást tenni arról, hogy a kódolás visszafejthetetlen volta az adott biometrikus sablon létrehozási módszerének egyszerű velejárója, vagy olyan kódolásról van szó, amely elősegíti a személyes adatok védelmére vonatkozó követelmények érvényesítését. Mindenesetre megállapítható, hogy a kódolás visszafejthetetlen volta nem szünteti meg az adat személyes adat jellegét.

4. Tudomása szerint a jogalkotó vizsgálta-e, hogy az alkalmazott kódolási technika valóban

visszafejthetetlen kódolást eredményez-e, illetve ezzel kapcsolatban készült-e szakértői vélemény, figyelemmel arra is, hogy korunk egyik komoly biztonsági kockázatot rejtő jelensége az elektronikus adatbázisok feltörhetőségének megakadályozása, és az ott tárolt adatok jogosulatlan felhasználása?

A Hatóságnak nincs tudomása arról, hogy a jogalkotó vizsgálta volna azt, hogy az alkalmazott kódolási technika valóban visszafejthetetlen információkat eredményez, illetve nincs tudomása vonatkozó szakértői vélemény elkészüléséről sem.

5. Milyen adatvédelmi kockázatát látja annak, hogy a biometrikus sablon egy külön adatbázisban tárolható?

A személyazonosság biometrikus ellenőrzése lehetséges központi biometrikus referencia adatbázis létrehozása és használata nélkül is. Példaként említhető az elektronikus tárolóelemet tartalmazó útlevél, melynek tárolója tartalmazza a személyazonosság ellenőrzéséhez szükséges biometrikus referencia sablonadatot. A személyazonosság ellenőrzésekor a biometrikus ellenőrző eszköz az érintettről az ellenőrzési eljárás során rögzített adat (arckép, ujjnyomat, íriszkép stb.) alapján elkészíti az illető biometrikus sablonját, majd összehasonlítja azt az útlevél elektronikus tárolóegységéből kiolvasott biometrikus referencia sablonadattal.

A fentiekhez képest a biometrikus személyazonosítás, illetve személyazonosság ellenőrzése céljából központi biometrikus adatbázis létrehozása a következő adatvédelmi kockázatokkal jár:

- A biometrikus azonosító adatok az érintett olyan fiziológiai, pszichológiai, magatartásbeli jellemzőit képezik le, amelyek közvetlenül kapcsolódnak az érintetthez, rá jellemzőek, állandóak, az érintett által rendszerint nem változtathatók meg és nem tagadhatók le. A hagyományos azonosító adatok közül például a név megváltoztatható, költözéssel a lakcím is, ám az arc vagy az ujjnyomat biometrikus azonosítás eredményét befolyásoló megváltoztatása sokkal nehezebb. Ezért az ilyen biometrikus adatokkal való visszaélés sokkal inkább veszélyes az érintett magánszférájának tiszteletben tartásához és személyes adatainak védelméhez való jogának érvényesülésére, mint az egyéb azonosító adatokkal való visszaélés.

- Ha a személyazonosság ellenőrzése a fenti példában ismertetett módon az érintett birtokában lévő elektronikus tárolóelemben tárolt biometrikus referenciaadatok felhasználásával történik, akkor az ellenőrzési eljárás során a rögzített, továbbá az elektronikus tárolóeszközből kiolvasott biometrikus adatok mindvégig a biometrikus ellenőrző eszköz zárt informatikai rendszerében maradnak és a felhasználást (a személyazonosság ellenőrzésének elvégzését) követően törlésre kerülnek. Ha ezzel szemben a személyazonosság ellenőrzéséhez központi biometrikus referencia adatbázist hoznak létre, akkor a biometrikus azonosító adatok kikerülnek az érintett birtokából, ezért többé nem lesz képes arra, hogy az adatok felhasználását közvetlenül ellenőrizze és megakadályozza a biometrikus adataival való visszaélést.

- A biometrikus azonosító adatok gépi feldolgozásra alkalmasak és egy részük – például az arckép vagy a járás, mozgás jellemzői – távolból, észrevétlenül az érintett tudta és közreműködése nélkül is rögzíthetők, ezért - ha rendelkezésre áll egy központi biometrikus referencia adatbázis és megfelelő számú, egységes rendszerebe kapcsolt közterületi képi megfigyelő eszköz (kamera) - elvileg alkalmasak az állampolgárok automatizált, tömeges, észrevételen azonosítását, megfigyelését végző informatikai rendszer létrehozására. Ezen technológiák kiterjedt, tömeges alkalmazása – ha a fejlődés eljut arra a szintre, hogy az azonosítás teljesen automatizálható - ahhoz vezetne, hogy a települési közterületek, a nyilvánosság számára nyitva álló egyéb közterületek és a tömegközlekedési eszközök teljesen megszűnnének a magánélet színterei lenni. Mindenkinek azzal kellene számolnia, hogy titokban folyamatosan, automatikusan megfigyelhetik. Ilyen helyzet kialakulása nyilvánvalóan sértené a magánélet tiszteletben tartásához és személyes adatok védelméhez fűződő jogot.

- A személyazonosításra alkalmas biometrikus sablon főszabályként olyan adat, amely közvetlenül, véglegesen, megváltoztathatatlanul és letagadhatatlanul kapcsolódik az adatalanyhoz. Ezért a személyazonosításra alkalmas biometrikus sablon a természete szerint egységes személyazonosító kód. Magyarországon az egységes és univerzális azonosító kód használata tilos. Ha létrejönne egy teljes népességre kiterjedő biometrikus referencia adatbázis, továbbá a központilag regisztrált biometrikus sablonon alapuló azonosítási mód alkalmazása általánossá válna, akkor e két körülmény együttes fennállása sértené az egységes és univerzális kód tilalmát, valamint az osztott információs rendszerekre vonatkozó alkotmányos követelményt.

6. Tudomása van-e arról, hogy a vényalenyomaton alapuló beléptetési rendszer bevezetése óta folytattak-e olyan vizsgálatot, amely azt ellenőrizte, hogy az adattárolás a Sporttv.-ben, illetve az Infotv.-ben (7. §) rögzített rendelkezéseknek megfelelően történik?

A Hatósághoz a vényalenyomaton alapuló beléptetési rendszer bevezetése óta csekély számú (összesen három darab) olyan bejelentés érkezett, amelyben az érintettek a Ferencvárosi Torna Club (a továbbiakban: FTC) által bevezetett biometrikus beléptető rendszer alkalmazásának jogalapját kifogásolták. A Hatóság ezekben az ügyekben mind azt állapította meg, hogy – tekintettel a Sporttv. módosítására – jogszabályi rendelkezések teszik lehetővé a klubok, így a az FTC-t az érintettek személyes és biometrikus adatainak kezelésére. A Hatóság ugyanakkor nem folytatott vizsgálatot és nincs is tudomása olyan eljárásról, amelynek tárgya a vényalenyomaton alapuló beléptetési rendszer keretében végzett adattárolásnak a Sporttv.-ben, illetve az Infotv.-ben (7. §) foglalt rendelkezéseknek való megfelelősége lett volna.

7. Az adatvédelmi biztos 2005.évi beszámolója szerint „a biometrikus azonosítás ma az, ami 15 évvel ezelőtt a távközlés, 10 évvel ezelőtt pedig az Internet volt". Mennyiben igazolja ezt az előrejelzést a biometrikus azonosítás adatvédelmi kockázataival összefüggő jelenlegi gyakorlata?

Az elmúlt évtizedben az informatikai rendszerek fejlődése, így különösen a számítógépes

tárkapacitások növekedése, az adatfeldolgozás gyorsulása, a hálózati adattovábbítási sávszélességek növekedése, valamint a különféle szenzorok fejlődése, továbbá a kapcsolódó költségek csökkenése lehetővé tette a biometrikus adatok feldolgozásán alapuló technológiák alkalmazásának tömeges elterjedését a piaci szférában és az állami adatkezelők esetében is.

A Hatóság eddigi tapasztalatai alapján a biometrikus rendszerek alkalmazása mind jobban elterjedőben van mind a világon, mind pedig Magyarországon. E rendszerek az érintettek magánszféráját nagymértékben, illetőleg az alkalmazott technológia természeténél, céljánál fogva nehezen megjósolható mértékben befolyásoló technológiák közé tartoznak. Emiatt a Hatóság számos esetben felhívta a közvélemény és a jogalkotók figyelmét a biometrikus adatkezelések veszélyire. A Hatóság továbbá az érintettek magánélet tiszteletben tartásához és személyes adatok védelméhez fűződő jogainak fokozottabb védelmét tartja szem előtt a saját eljárásai során is.

2012-ben és 2013-ban több konzultációs megkeresés is érkezett a Hatósághoz azzal kapcsolatban, hogy bizonyos adatkezelők milyen feltételek mellett alkalmazhatnak biometrikus rendszereket az ügyfeleik azonosítása céljából. A Hatóság a beadványok megítélése szempontjából irányadónak tekintette az Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (a továbbiakban: Munkacsoport) által elfogadott, a biometrikus technológiák terén történt fejleményekről szóló 3/2012. számú vélemény (WP193)[1] útmutatásait. A Munkacsoport e dokumentumban kifejtette, hogy a biometrikus rendszerek alkalmazása felveti az arányosság kérdését a feldolgozott adatok tekintetében. Mivel a biometrikus adatok csak akkor kezelhetők, ha megfelelőek, relevánsak és nem túlzott mértékűek, ezért minden esetben mérlegelni kell a kezelt adatok szükségességét, arányosságát, valamint azt, hogy az adatkezelés által elérni kívánt cél megvalósítható lenne-e a magánszférát kevésbé korlátozó módon. Ennek megfelelően egy tervezett biometrikus rendszer „arányosságának elemzése során előzetesen mérlegelni kell, hogy a rendszer szükséges-e a meghatározott igény kielégítéséhez, azaz használata elengedhetetlen-e ehhez, vagy inkább annak legkényelmesebb vagy legköltséghatékonyabb módja. Egy második megfontolandó tényező az, hogy a rendszer valószínűleg elég hatékony lesz-e az adott igény kielégítésében, tekintettel a használni tervezett biometrikus technológia sajátos jellemzőire. A harmadik mérlegelendő szempont, hogy arányos-e az elvárt előnyökkel, ha a rendszer miatti sérül a magánélet védelme. Ha az előnyök viszonylag kisebbek, például kényelmesebb az eljárás vagy kismértékű költségmegtakarítás érhet ő el, akkor nem helyénvaló, ha sérül a magánélet védelme. Egy biometrikus rendszer megfelelőségének értékelése során a negyedik szempont annak megfontolása, hogy a magánéletbe kisebb mértékben beavatkozó módszerek elérhetnék-e a kívánt célt". A Hatóság a fenti szempontok figyelembe vételével alakította ki állásfoglalásait a hozzá érkezett megkeresésekkel kapcsolatban.

Az egyik esetben egy gyermekfogászati szakrendelését ellátó fogászati központ kért állásfoglalást a Hatóságtól arról, a szakrendelésre érkező gyermek azonosítását megoldhatnák-e egy ujjlenyomat-alapú biometrikus azonosító rendszer üzembe helyezésével, amely kiváltaná az érintett páciensek papíralapú azonosítását. A Hatóság ebben az ügyben kifejtette, hogy a fogászati központ által bevezetni kívánt ujjlenyomat alapú azonosítási rendszer nem elengedhetetlen a tevékenységének végzése szempontjából, mivel az csupán az ügyfelek fogadását teszi kényelmesebbé (NAIH-6300-2/2012/V.).[2]

A Hatósághoz érkezett olyan beadvány is, amelyben egy viszonylag elterjedt módszer, az ujjlenyomat-alapú azonosítást kívánták pénztárgépeknél alkalmazni abból a célból, hogy ahhoz csak az arra jogosult munkavállalók férhessenek hozzá. A Hatóság a Munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 9-10. §-aira tekintettel kifejtette ezzel kapcsolatban,

hogy a munkáltató oldalán fennáll az a védendő érdek, miszerint az általa üzemeltetett pénztárgép biztonságos legyen, abból pénzt csak az arra feljogosított munkavállaló vagy munkavállalók vehessenek ki. A pénztárgéphez való hozzáférés korlátozása ezért – általánosságban – megfelel az objektív szükségesség kritériumának. Az objektív szükségesség követelményén túl az Mt. továbbá megfogalmazza az arányosság kritériumát is, amelynek tekintetében az Adatvédelmi Munkacsoport már említett Véleményében foglaltak az irányadók. Az említett szempontok figyelembe vételével a Hatóság megállapította, hogy az ujjlenyomat-azonosítás alapú pénztárgép alkalmazása nem felel meg az arányosság követelményének, mivel az általa elérni kívánt előnyök más, a személyhez fűződő jogokat kevésbé korlátozó módszerek segítségével is elérhetőek. Ilyen lehet például az olyan fokozott biztonságú pénztárgép alkalmazása, amelyhez csak egy előre meghatározott, és kizárólag a munkáltató, illetőleg az arra feljogosított munkavállalók által ismert kóddal lehet hozzáférni.[3]

A Hatóság egy magánszemély által tett bejelentés nyomán az érintettek személyes adatok védelméhez fűződő jogának súlyos sérelmét állapította meg abban az ügyben, amelyben egy állampolgár azt kifogásolta, hogy a Semmelweis Egyetem ÁOK Szemészeti Klinika (a továbbiakban: Klinika) olyan ujjnyomat-azonosítás alapján működő biometrikus beléptető rendszert helyezett üzembe, amelynek kizárólagos célja a munkaidő betartásának ellenőrzése. A vizsgálat eredményeként a Hatóság egyrészt megállapította, hogy a munkaidő nyilvántartás nem minősül olyan célnak, amelynek elérése érdekében a biometrikus rendszer elengedhetetlenül szükséges lenne. Másrészt azt hangsúlyozta, hogy a megfelelő alternatívák hiányának követelménye csak abban az esetben teljesül, ha valóban nem létezik más olyan módszer, amely kevésbe valósítana meg beavatkozást 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. A Hatóság ezért felszólította a Klinikát arra, hogy haladéktalanul szüntesse meg a biometrikus rendszer keretében végzett adatkezelést.

Fontosnak tartjuk, hogy a jogi szabályozás ne maradjon le a gyors technológiai változások mögött. Az államnak kitüntetett felelőssége van abban, hogy a biometrikus adatkezelés elterjedése ne veszélyeztesse a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő jogot, ezért Hatóságunk 2014-ben az igazságügyi miniszternél, valamint a belügyminiszternél kezdeményezte a biometrikus adatkezeléshez kapcsolódó adatvédelmi szabályrendszer megalkotását. Az egységes jogi normák egyrészt megkönnyítenék a jogalkalmazók munkáját. Másrészt a jogszabályi definíció és az átfogó szabályozás nagyban hozzájárulna a biometrikus rendszerek alkalmazásával összefüggő állampolgári tudatosság növeléséhez is. A Hatóság emellett megfontolandónak tartja azt is, hogy a hazai törvényi keretek között a biometrikus adatok kiemelt védelemben részesüljenek. Az Adatvédelmi Hatóságok Európai Konferenciáján 2014. június 5-én elfogadott határozat a biometrikus adatoknak a különleges adatok kategóriájában történő besorolását javasolta.[4] Ezt a javaslatot a Hatóság is átvette az igazságügyi miniszterhez eljuttatott biometrikus adatok kezelésével kapcsolatos ajánlásában.

8. Álláspontja szerint mennyiben befolyásolja a biometrikus azonosítási rendszer adatvédelemmel összefüggő megítélését a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet) szóló uniós jogalkotási folyamat? Figyelemmel különösen arra, hogy az Európai Parlament és Tanács COM (2012) 11 final szám alatt közzétette azt a rendelet-tervezetet, amelynek az elfogadását követően a közvetlen hatály érvényesülése folytán a személyes

adat és a biometrikus adat fogalma az Európai Unió területén egységessé válik. Ez utóbbi pedig „az egyén olyan fizikai, pszichológiai vagy viselkedési jellemzőjére vonatkozó adat, amely lehetővé teszi az egyedi azonosítását, mint például arckép vagy a daktiloszkópiai adat".

A Hatóság több fórumon is kifejtette azon álláspontját, miszerint eljött az ideje a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv (a továbbiakban: Irányelv) felülvizsgálatának és egy új, egységes európai uniós adatvédelmi szabályozás kialakításának.[5] A Hatóság ezért kifejezetten üdvözölte, hogy az Európai Parlament és Tanács COM (2012) 11 final szám alatt közzétett rendelet-tervezete több szempontból is jelentős és előremutató változásokat javasol az adatvédelem közösségi szabályozása terén.[6] A rendelet-tervezet azonban még csak javaslati formában létezik, az Európai Parlament, illetőleg a Tanács csak 2015 őszén veszi napirendjére. Ezt követően indul meg az egyes rendelkezésekkel kapcsolatos vita. A jogalkotónak továbbá meg kell fontolnia a rendelet-tervezetéhez benyújtott rendkívüli mennyiségű módosító javaslatot is. Az európai uniós jogalkotási folyamat végén a Hatóság reményei szerint egy szigorú, de az információs társadalom jelentette kihívásoknak megfelelő rendelet fog születni.

Tekintettel a jogalkotási folyamat jelenlegi állására, a Hatóság az új rendelet konkrét, a biometrikus azonosítási rendszer adatvédelmi megítélését befolyásoló tartalmával kapcsolatban még nem tud kielégítő felvilágosítást adni Önnek. A vonatkozó kérdésekkel összefüggésben esetlegesen tájékoztatást nyújthatnak Önnek Magyarország európai parlamenti képviselői, illetőleg az Igazságügyi Minisztérium. Az Európai Parlament tagjai, illetőleg a minisztérium ugyanis közvetlenül részt vesznek, illetőleg figyelemmel kísérik a rendelet-tervezet elfogadásának folyamatában.

9. Fenntartja-e a Sporttv. módosításáról szóló 2014. évi XXVII. törvény normaszöveg-javaslatához – az Infotv. 38. § (4) bekezdés a) pontja alapján – tett észrevételében foglaltakat?

A Hatóság továbbra is fenntartja a NAIH-1387-2-2014-J. számon kelt véleményben foglaltakat.[7] Az említett dokumentumban több szempontból is komoly kritikákat fogalmazott meg az országgyűlés elé került törvényjavaslattal összefüggésben. Ezek közül a legfontosabbak az következőképpen foglalhatók össze.

A Hatóság – az Infotv. 4. § (2) bekezdésére tekintettel – kifejtette, hogy a törvényjavaslat, illetőleg a jelenleg hatályos Sporttv. értelmében az érintettek azonosítására több – eltérő adatkörön alapuló – lehetőség is rendelkezésre áll. Ebben a tekintetben tehát nem érvényesül megfelelő módon az adatminimalizálás elve. Az adatminimalizálás alapelve értelmében csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulása szempontjából elengedhetetlen, a cél elérésére alkalmas, kizárólag a cél megvalósulásához szükséges mértékben és ideig. Ezen alapelv figyelembe vétele szavatolja, hogy az adatkezelés céljára tekintettel csupán a legszűkebb, indokolt adatkör kezelésére kerül sor. Az adatminimalizálás elve továbbá kizárja a készletezésre történő adatkezelést, azaz hogy olyan adatok felvételére kerüljön sor, amelyeket csak később meghatározásra kerülő célból gyűjtenek. A törvényjavaslat, illetőleg a jelenleg hatályos Sporttv. értelmében azonban az érintettek azonosítására több – eltérő adatkörön alapuló – lehetőség is rendelkezésre áll. Ebben a tekintetben tehát nem érvényesül megfelelő módon az

adatminimalizálás elve. Amennyiben ugyanis az érintett rendelkezik az azonosításához szükséges okirattal, feleslegessé válik a további azonosítási módok kötelező előírása.

A Hatóság felhívta továbbá a jogalkotó figyelmét arra is, hogy az ún. privacy by design szemléletnek megfelelően az adatkezelő köteles a működését, struktúráját az adatvédelmi szempontok maximális figyelembevételével kialakítani. Az Infotv. 7. § (1) bekezdése ezzel összhangban úgy rendelkezik, hogy az adatkezelők kötelesek az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsák az érintettek magánszférájának védelmét. A Spottv.-ben foglalt biometrikus beléptető rendszer kialakításával kapcsolatban ez azt jelenti, hogy az adatkezelőknek olyan rendszerek bevezetésére kell törekednie, ennek megfelelően pedig a törvényalkotónak olyan jogszabályi környezetet kell kialakítania, amelyek szem előtt tartják az érintettek magánélet tiszteletben tartásához és személyes adatok védelméhez fűződő jogát. Figyelembe véve a korábbi adatvédelmi biztosi gyakorlatot, a Hatóság álláspontja szerint az biztosította volna a legmagasabb szinten az említett alapjogok érvényesülését, amennyiben az érintettek biometrikus sablonjait az általuk birtokolt klubkártyán elhelyezett adathordozón tárolnák. A biometrikus beléptető rendszer pedig a kártyán lévő letárolt biometrikus sablont helyben hasonlítaná össze az érintett tenyeréről képzett sablonnal. E megoldás több ok miatt is különösen előnyös lett volna. Egyrészt az érintett nemcsak a biometrikus adata, hanem a biometrikus sablon felett is gyakorolhatja információs önrendelkezési jogát. Másrészt az adatkezelő egyetlen adatkezelési műveletet leszámítva nem kezelné fizikailag a biometrikus sablonokat, hiszen azokat a biometrikus beléptető rendszer dolgozná fel automatikusan. Emiatt viszont az adatkezelőnek sem kellene külön nyilvántartást fenntartani a biometrikus sablonok számára, és így jelentős mértékben csökkenteni lehetne az adatvédelmi és adatbiztonsági követelményeknek való megfelelés szempontjából rá háruló anyagi és más terheket is. Harmadrészt pedig az érintett és a klubkártyán tárolt személyes adatok közötti kapcsolatot az összepárosított biometrikus sablonok teremtenék meg, azaz a rendszer biztonságának szintje nem csökkenne, hiszen az érintett biometrikus adata, vagy a letárolt biometrikus sablont tartalmazó klubkártya hiányában továbbra sem lenne lehetséges belépni a sportlétesítmény területére. A klubkártya esetleges elvesztése továbbá nem jár azzal a – hagyományos mágneskártyás beléptető rendszerek esetében gyakran hangoztatott – veszéllyel, hogy az érintett helyett, annak személyes adataival visszaélve egy harmadik személy lép be az adott területre. Az adatalany biometrikus adatából képzett biometrikus sablon ugyanis annyira egyedi és hamisíthatatlan, hogy a rendszer nagy pontossággal meg tudja különböztetni a belépésre nem jogosult személyt az arra jogosulttól. Az adathordozó programozása és elhelyezése a klubkártyákon pedig nem jár jelentősebb többletmunkával, illetőleg kiadásokkal.

A Hatóság végül kitért arra, hogy a törvényjavaslat indokolása csupán általánosságban határozza meg azt a célt („a sportesemény szervezők a modern technológia segítségével már beléptetésnél kiszűrhessék azokat, akik korábbi rendzavarásukkal veszélyeztették a fair play szellemét a lelátókon"), amelynek érdekében a biometrikus beléptető rendszer bevezetésre kerülhet. Az Infotv. 4. § (1) bekezdése értelmében ugyanakkor személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. A Munkacsoport a célhoz kötöttségről szóló 03/2013. számú véleményében (WP203)[8] kifejtette, hogy az adatkezelés céljának meghatározása a személyes adatok védelme jogi szabályozásának középpontjában áll. Azon cél meghatározása ezért, amelynek érdekében az adatkezelés történik, szükséges előfeltétele annak, hogy megállapítható legyen az adatkezelés jogszerűsége, illetőleg az alkalmazandó adatvédelmi garanciák. Az adatkezelés célját világosan és egyértelműen meg kell határozni: részletesen meg kell adni ahhoz, hogy megállapítható legyen, hogy milyen típusú adatkezelési művelet kapcsolódik az adott célhoz, és hogy melyik nem. A biometrikus adatok tekintetében ez azt jelenti, hogy –

többek között – figyelembe kell venni a Munkacsoport 3/2012. számú véleményében foglaltakat is. E szempontok mérlegelését az adatkezelő, illetőleg – kötelező adatkezelés esetén – a jogalkotó köteles elvégezni. Ennek keretében többek között megfelelő módon fel kell mérni, hogy a javaslat részletes indokolásában említett személyiséglopás (a korábban rendbontást elkövető személyek más személyazonosságával lépnek a stadionok területére) valóban olyan konkrét, folyamatos és jelentős kockázatot jelent, amely megalapozza a biometrikus beléptető rendszer alkalmazásának szükségességét. Amennyiben nincsen ilyen, az adatkezelés szükségességét és arányosságát alátámasztó indok, a javaslat, illetőleg a jelenleg hatályos Sporttv. nem feltétlenül felel meg az alkotmányossági követelményeknek.[9]

Budapest, 2015. augusztus „10".

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

1 ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf.

2 www.naih.hu/files/NAIH_BESZaMOLo_2012_net3.pdf.

3 www.naih.hu/files/NAIH-beszamolo2013--MID-RES.pdf.4 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/14-06-05_Strasbourg_resolution_1_EN.pdf.

5 http://orientpress.hu/118568.

6 http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52012PC0011&qid=1438609925591&from=EN.

7www.naih.hu/files/NAIH-1387-2-2014-J-140606.pdf

8 ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf#h2-2.

9 Az Alkotmánybíróság például kifejezetten hangsúlyozta a 26/2014. (VII. 23.) AB határozatban, hogy a választási eljárásról szóló 2013. évi XXXVI. törvény 2. § (4) bekezdésének indítványozók által támadott második mondata