NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
SZAKÉRTŐI INTÉZET

1399 BUDAPEST 62. Pf.: 710/3.
Telefon: 325-7672, Fax: 391-1804

SZAKÉRTŐI VÉLEMÉNY

IV/6/2015.

..... számú ügyben

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
SZAKÉRTŐI INTÉZET
1399 BUDAPEST 62 Pf.: 710/3.

2...sz.pld.

Ikt.sz.: 30700/0/13623/2/2016.

Tárgy: szakértői vélemény
Hiv. szám: IV/6/2015.

OKMÁNYBIZTONSÁGI ÉS INFORMATIKAI EGYESÍTETT SZAKÉRTŐI VÉLEMÉNY

Készült: Az **Alkotmánybíróság** előtt IV/6/2015. sz. alatt, a sportról szóló 2004. évi I. törvény (a továbbiakban: Sporttv.) egyes rendelkezései alaptörvény-ellenességének megállapítása és megsemmisítése iránt benyújtott alkotmányjogi panasz folytán megindult eljárásban.

A vizsgálat tárgya:

Az ügyben az alapjogi jogsérelem fennállásának eldöntése érdekében informatikai biztonsági szakkérdés tisztázása.

A szakértőnek átadott anyagok:

- a szakértő kirendelő végzés 1 példánya
- az alkotmányjogi panasz 1 munkapéldánya
- az FTC Labdarúgó Zrt. amicus curiae beadványának 1 munkapéldánya

A szakértői vizsgálat folyamata

Megállapítottuk, hogy a szakkérdések megválaszolásához szakértői módszertant nem szükséges alkalmazni, azonban a Tisztelt Alkotmánybíróság döntéshozatalának elősegítése érdekében elengedhetetlenül fontosnak tartottuk a kérdésekhez kapcsolódó technikai fogalmak pontosítását, magyarázatát. Különös tekintettel arra, hogy a beadvány tárgyát képező, sportról szóló törvény kodifikálásakor nagy valószínűséggel nem vették igénybe informatikai szakember segítségét. Ebből fakadóan a törvény vonatkozó szövege (72/A.§) szakmai szempontból pontatlan, e miatt nem egyértelmű.

A biometrián alapuló azonosító rendszerek tárgyköre szerteágazó és a nem szakember számára meglehetősen bonyolult. Ezért – ahol lehetséges volt – megpróbáltuk köznapi példákkal érthetőbbé tenni a szakmai nyelvezetet.

Az ügyben érintett fogalmak

Hash

A kirendelő végzésben többször említésre kerül a T/156. számú törvényjavaslat eredeti normaszövegében szereplő „HASH-kód" kifejezés, amely egy oximoron, vagyis olyan gondolatalakzat, amely egymást kizáró, egymásnak ellentmondó fogalmakat foglal szoros gondolati egységbe. A „hash" nem mozaikszó (ezért nem csupa nagybetűvel írandó), hanem a *hash function* vagy *hash value* angol kifejezésekre utaló szó, amelyeknek magyar megfelelőjük rendre a **hasítófüggvény**, illetve a **hasítóérték** szakkifejezések.

A hasítófüggvények az informatikában használt speciális eljárások, amelyek tetszőleges hosszúságú bemeneti adatot megszabott hosszúságú kimeneti adattá alakítanak. **A hasítófüggvények egyirányú függvények, kimeneti adatuk a hasítóérték** (*hash value*), amelyet a köznyelv tévesen „hash kódnak", illetve „hash kulcsnak" is nevez. A hasítófüggvények rövid egyedi azonosítók előállítására alkalmasak, különböző felhasználási célokra. Az önmagában említett „hash" kifejezésből nem derül ki, hogy hasító eljárásról (hasítófüggvény), vagy annak eredményéről (hasítóérték) van-e szó.
Egyszerű hasonlattal élve egy hasító algoritmussal végzett művelet eredménye lehet az is, ha például egy nyomda az általa kiadott könyvek ISBN számát az egyes könyvek első 64 oldalán található első betűkből képzett karaktersorozat alapján képezné és tartaná nyilván. Ez megkönnyíti az egységes nyilvántartást és keresést, mivel minden könyv egyetlen, de könyvenként eltérő, mindig azonos hosszúságú adat segítségével azonosítható. Ebben az esetben tehát **a hasítóérték az eredeti adat** (könyv) **szeleteit képezi, amely adatszeletek közvetlenül is olvashatóak maradhatnak.**

Belátható, hogy lehetséges, de kevéssé valószínű olyan könyvet találni, amelynek oldalain a kezdőbetűk sorrendje megegyezik, ami a hasító algoritmus kimeneti értékének (hasítóértékének) azonosságához vezet. Függvényekkel végzett műveletek során előfordulhat az is, hogy különböző bemeneti értékekhez ugyanaz a kimeneti érték tartozik, így elképzelhető, de – jól megválasztott függvény esetén – kevéssé valószínű több olyan különböző tartalmú könyv létezése, amelyeknek az ilyen módon előállított hasítóértéke véletlenül megegyezik. A hasító algoritmus alkalmazása tehát azért előnyös, mert egy könyv azonosításához nem a könyv teljes tartalmát kell összevetni a többi könyv teljes tartalmával (ami rendkívül időigényes folyamat lehet), hanem csak a könyvek tartalmából képzett rövid, tömör hasítóértékeket.

A példában említett hasító algoritmus tehát alkalmas lehet a könyv egyedi azonosítására, azonban a könyv teljes tartalma a hasítóértékből nem állítható helyre. A biometrikus adatokból is hasító algoritmusok segítségével képezik le a biometrikus sablont. **Az eredeti (nyers, feldolgozatlan) biometrikus adat** (a méréssel rögzített ujjnyom, vénatérkép, stb.) tehát **a biometrikus sablonból nem állítható helyre maradéktalanul, de a biometrikus sablon továbbra is alkalmas marad a személyazonosításra.**

A kriptográfiai hash

A kriptográfiai hasítófüggvények ezzel szemben szándékosan helyreállíthatatlan és felismerhetetlen módon képezik le az eredeti adatot. A kriptográfiai hasítófüggvény gyakorlatilag nem invertálható függvény, vagyis a hasítóértékből gyakorlatilag lehetetlen helyreállítani az eredeti adatot. Kriptográfiai hasítófüggvény esetében **a hasítóérték minden esetben a teljes adattartalomból képződik**, ezért **egyetlen bitnyi információ megváltoztatásával is jelentősen különböző hasítóértékek keletkeznek**. Ez a tulajdonságuk lehetővé teszi, hogy a kriptográfiai hasítófüggvény segítségével **az eredeti adat tárolása nélkül**, mégis **az eredeti adatra jellemző lenyomatot** (vagy ha úgy tetszik, sablont) lehessen képezni.

Hasonlatunkhoz visszatérve, egy kriptográfiai hasítófüggvény segítségével két különböző tartalmú könyv teljes adattartalmából képzett kriptográfiai hasítóértékek akkor is eltérőek lesznek, ha történetesen a két könyv első 64 lapján található első betűk véletlenül megegyeznek. **A kriptográfiai hasítóértékek** megjelenésükben tehát **nem tartalmaznak** az oldalak **eredeti tartalmával egyező adatokat, mégis alkalmasak egyedi azonosításra. Ha** azonban a könyvben akár egyetlen betűt (vagy írásjelet, ékezetet stb.) megváltoztatunk, vagyis **az adattartalom bitre pontosan nem egyezik meg, akkor a kriptográfiai hasítóérték megváltozik.**

nnak ellenére, hogy **a kriptográfiai hasítófüggvény** segítségével képzett kriptográfiai ısítóértékből az eredeti adat nem olvasható ki, az eljárás **mégsem nevezhető titkosításnak**, gyanis **a titkosító eljárások lényegi eleme a kétirányúság**, vagyis a titkosított szöveget a tkosító algoritmus és/vagy a kulcs(ok) ismeretében egyértelműen újra olvashatóvá lehet alakítani. riptográfiai hasítófüggvények esetében ez nem teljesül, ugyanis a végtelenből (tetszőleges osszúságú bemeneti adatból) végesbe (megszabott hosszúságú hasítóértékbe) történő leképzés iatt szükségszerű, hogy a bemeneti adat a kimenet alapján eredetben nem állítható helyre. **Eltérő emeneti adattartalom is eredményezhet azonos hasítóértéket, azonban** ennek **matematikai alószínűsége kellően csekély** ahhoz, hogy a kriptográfiai hasítófüggvények a gyakorlatban lkalmazhatóak legyenek kriptográfiai célokra.

lasítóértékek esetében a **kód** megnevezés azért nem helytálló, mert a kommunikációban és az nformáció feldolgozásban a kódolás egy olyan eljárást jelöl, amit egy forrás objektumon égrehajtva az információt adattá alakítja, amely aztán elküldhető egy adatfeldolgozó rendszernek, mely visszaállítja az eredeti információvá. A kódolt adat (vagyis a kód) visszaállítási eljárása a ekódolás, amely során a forrás által elküldött adat a vevő számára értelmezhető, az eredetivel zonos információvá kerül visszaalakításra. Ebben az értelemben tehát **a hasítófüggvények imenete nem kód**, mivel **a hasítóértékből az eredeti adattartalom gyakorlatilag nem elyreállítható**, hiszen pontosan ez a tulajdonság a kriptográfiai hasítófüggvények lkalmazhatóságának lényege. **A „hash-kód" tehát értelmetlen szóösszetétel.**

z eddig megismerteket összefoglalva tehát:

hasítóérték

- az eredeti adattartalommal csak egy irányban megfeleltethető,
- nem titkosított, az adat eredeti megjelenési formájának egyes részleteit tartalmazó,
- az eredeti adat részleges elvesztésével járó,
- hasítófüggvény algoritmusa által előállított,
- jellemzően hexadecimális formában megjelenített bináris (gépi kódolású) adat.

speciálisan megválasztott hasító algoritmusok alkalmasak a biometrikus azonosító rendszerekben asznált biometrikus sablonok készítésére, hiszen a hasítóérték képzése során ugyan az eredeti adat lentős része elveszik, de egyes, azonosításra alkalmas jellemzői megmaradnak.

kriptográfiai hasítóérték

- az eredeti adattartalommal csak egy irányban megfeleltethető,
- nem titkosított, de az adat eredeti megjelenési formáját elrejtő,
- az eredeti adat teljes elvesztésével járó,
- kriptográfiai hasítófüggvény algoritmusa által előállított,
- jellemzően hexadecimális formában megjelenített bináris adat.

A kriptográfiai hasítófüggvények lényegüknél fogva alkalmatlanok a biometrikus azonosító rendszerekben használt biometrikus sablonok készítésére, mert a mérési adatok szórása miatt sohasem keletkezik két bit-azonos biometrikus adat. Ennél fogva a belőlük képzett kriptográfiai hasítóértékek is mindig jelentősen eltérőek, összehasonlításra alkalmatlanok lesznek. A kriptográfiai hasítófüggvényeket ezért csak bit-azonos adatok rejtésére és/vagy összehasonlítására alkalmazzák (pl. jelszavas hitelesítés, adathordozók adattartalmának hitelesítése, stb.)

kódolt adat (kód)

- az eredeti adattartalommal mindkét irányban megfeleltethető,
- nem titkosított, de az adat eredeti megjelenési formáját adatátvitel vagy adatfeldolgozás céljából megváltoztató,
- az eredeti adattartalom megőrzésével járó,
- kódoló algoritmus által előállított, dekódoló algoritmus által visszafejthető,
- a kódolási eljárástól függő formában megjelenített adat.

A kódolási eljárások alkalmasak az adat megjelenítési formájának megváltoztatására, és visszaalakítására. Célja nem a titkosítás, hanem az adat továbbítására, tárolására, illetve feldolgozására alkalmas formátumra való alakítás (pl. Morse kód, ASCII kód, stb.).

A titkosított/rejtjelezett adat (rejtjel)

- az eredeti adattartalommal mindkét irányban megfeleltethető,
- az adat eredeti megjelenési formáját megváltoztató és elrejtő,
- az eredeti adattartalom megőrzésével járó,
- titkosító algoritmus által előállított és a titkosító kulcs(ok) ismeretében visszafejthető,
- a visszafejtéshez szükséges speciális tudással nem rendelkező fél számára olvashatatlan formában megjelenített adat.

A titkosítási eljárások alkalmasak az adat bizalmasságának megőrzésére, vagyis az illetéktelenek számára megismerhetetlenné, az illetékesek számára pedig olvashatóvá tételére (pl. AES-192, RSA-2048, ECC-256, stb.).

Biometria

A biometria olyan általános fogalom, melyet két értelemben is használnak:

- a személyek valamely fiziológiai vagy viselkedésbeli jellemzőinek mérését, és/vagy
- a fenti mérési adatokon alapuló automatikus személyazonosítást jelenti.

Az alkalmazható biometriai jellemzők köre az ilyen irányú tudományos kutatások kiterjedésével folyamatosan bővül. Néhány példa a biometriai azonosításra alkalmas jellemzőkre:

- Fiziológiai (statikus)
  - arcgeometria,
  - ujjlenyomat,
  - kézgeometria,
  - vénatérkép,
  - íriszfelépítés,
  - szemfenék érstruktúra;
- Viselkedésbeli (dinamikus)
  - járás,
  - billentyűzet-kezelés,
  - beszédhang
  - aláírás.

biometria alkalmazása

biometria alkalmazására az egyértelmű, mérési adatokon alapuló személyazonosítás grehajtásához van szükség. Az alkalmazott biometriai módszer kiválasztásának szempontjaira nkrét előírások nem léteznek. Az alábbi megfontolásokat érdemes figyelembe venni a ometrikus rendszer kiválasztásánál:

- szükséges és elégséges beavatkozás a személyazonosság megállapítása érdekében (technikai-biológiai behatolás a magánszférába);
- mit akarunk védeni a biometriai azonosítással (minél fontosabb a védendő dolog, annál fontosabb a legpontosabb azonosításra törekedni);
- társadalmi elfogadottság szintje (arckép, ujjlenyomat);
- praktikusság (beléptető rendszer a szükséges pontossággal, gyorsasággal működik-e);
- tartósság stb.

lérés (metria)

ervszerűen végrehajtott gyakorlati tevékenységek összessége, amely valamely fizikai, kémiai stb. ennyiség nagyságának, arányának jellemzésére alkalmas. A mérés számszerűsítéséhez érőeszközt használunk. **A helyes mérés előfeltétele a mérés reprodukálhatósága. Ez azonban em mindig jelenti azt, hogy egy adott mérést megismételve ugyanazt az értéket kapjuk.** A érési eredmények a gyakorlatban bizonyos mértékű szórást mutatnak. A szórás a mérés izonytalanságából ered. A bizonytalanságot több tényező is befolyásolja. Ilyenek lehetnek, a érést zavaró zajok, a mérőeszköz hibája, a leolvasás pontatlansága, számolás során alkalmazott erekítések, stb.

biometrikus adatok mutatnak ugyan állandó jellemzőket, de a mérésük során számos életlenszerű tényező, mérési zaj (ujj pozíciója a leolvasó-felületen, szennyeződések az ujjon, rckifejezés, arcszőrzet, fényviszonyok, stresszhelyzet stb.) befolyásolja az egyszeri mérés során inyert adatokat.

iometrikus sablon

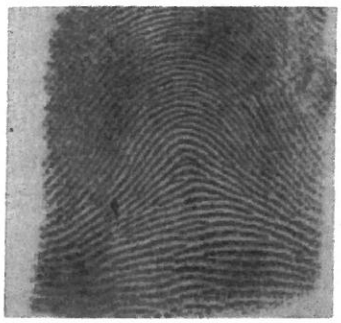
biometrikus sablon *(template)* egy **biometriai jellemzőnek egyszerűsített, gépi kódolású egjelenése**, melyet (az esetek túlnyomó többségében szabadalmaztatott) számítógépes lgoritmussal állítanak elő és lehetővé teszi egy külön eljárásban rögzített azonos jellemvonás zonos algoritmussal képzett sablonjával való összevetés elvégzését annak érdekében, hogy **az gyezés mértéke megállapításra** kerülhessen.

biometrikus sablon tipikusan egy viszonylag kisméretű adat. Minden biometrikus azonosítást iztosító rendszer előállítója egyedi sablon formátumot alkalmaz, ezért azok a különböző endszerek között nem kicserélhetők.

biometrikus sablon alkalmazásának mindössze az a célja, hogy a rendszerint részletes, nagy onyolultságú és ezért nagy méretű biometrikus adatból **az adatfeldolgozó rendszer számára önnyen kezelhető, kis méretű, ezért tárolásához és feldolgozásához kevesebb erőforrást génybe vevő formátumot** alkalmazzanak a biometrikus jellemzők automatizált összevetése során.

biometrikus sablon nem eredetben tárolja a biometrikus adatot, hanem csak a vett minta szehasonlítására alkalmas jellemzőket tárolja. Ujjnyom esetében például a biometrikus sablon a rfodorszál-rajzolatok meghatározott pontjaiban (minúcia) a fodorszál irányát rögzíti, amely ányvektorok segítségével nagyjából rekonstruálható és összehasonlítható más mintázatokkal.

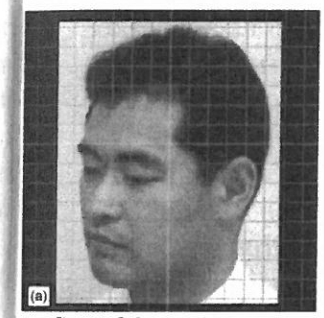
ldák biometrikus adatból leképezett biometrikus sablonokra:



a) egy ujjnyomat beolvasott képe, vagyis a biometrikus adat

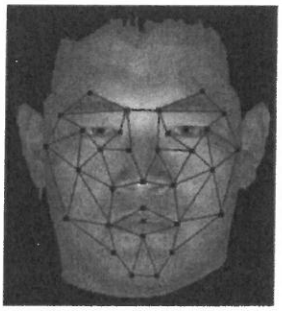
b) az ujjnyomatból leképezett 2D biometrikus sablon

c) a biometrikus sablonból helyreállítható stilizált ujjnyomat

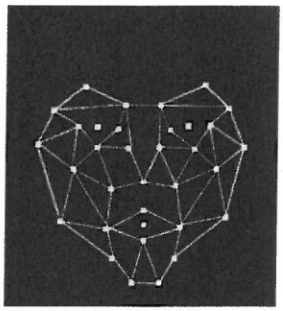


d) arckép, mint biometrikus adat

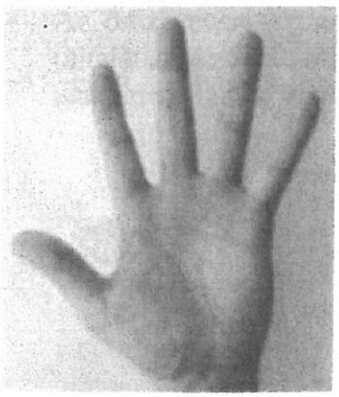
e) mérési pontok felvétele



f) arcjellemzőket leíró pontrács illesztése



g) arcképből leképezett 3D biometrikus sablon



h) tenyér fényképe

i) a tenyér infravörös fényű megvilágításban készített képe, mint biometrikus adat

j) az infravörös megvilágítású tenyér vénalenyomatából képzett biometrikus sablon

A biometrikus sablon tehát mérhető jellemzőket tartalmazó bináris adathalmaz, amelynek datstruktúrája teljes mértékben a mérni kívánt biometrikus jellemzőtől, illetve annak absztrahációs nódszerétől függ. A tárolás formátuma (vagy kódolása) irreleváns, de az illetéktelen hozzáférés llen a sablonok adattartalmát – személyes adatról lévén szó – valamilyen titkosítási eljárással édeni kell.

sablonokat alkalmazó biometrikus azonosító rendszerek tehát nem a helyszínen beolvasott ometrikus adatot (képmás, ujjnyomat, íriszkép, vénalenyomat, stb.) vetik össze az adatbázisban gy chipkártyán tárolt mintákkal, hanem a helyszínen beolvasott biometrikus adatból azon omban leképezett biometrikus sablon adattartalmával vetik össze az adatbázisban vagy ipkártyán tárolt biometrikus sablonok adattartalmát.

iometrikus sablon alkalmazása azonban nem minden esetben célszerű, bizonyos felhasználási lokra (például a biometrikus azonosító és nyilvántartó rendszerek közötti kompatibilitás egőrzése érdekében) közvetlenül a biometrikus adat kerül tárolásra és összehasonlításra (pl. útlevélben vagy eSZIG-ben tárolt ujjlenyomat). Tekintve, hogy mind az eredeti biometrikus adat, ind pedig a belőle képzett biometrikus sablon alkalmas a személyazonosításra, jogi és latvédelmi szempontból lényegtelen a sablon alkalmazása, vagy annak hiánya, mivel az adatok emélyhez köthetőségének tényén nem változtat.

biometrikus azonosító rendszerek működési elve

rendszer kialakítása a következő főbb lépések végrehajtásával történik:

- A személyazonosság hiteles megállapítása – biztosítja, hogy a rendszerbe bekerülő személy kétség nélkül ismert;
- A biometrikus adat rögzítése – a nyers (átalakításra még nem került) biometrikus adat felvétele;
- Kivonás, illetve szükség esetén sablonkészítés – a nyers biometrikus adatból mérhető adatok előállítása és azok sablonná alakítása, tárolása;
- Amennyiben a rendszer biometrikus sablonokat használ az azonosítás céljára, akkor utólag a nyers biometrikus adat – mivel az azonosítási eljáráshoz már nem szükséges – törlésre kerül a rendszerből; ellenkező esetben maga a biometrikus adat kerül rögzítésre a későbbi összevetés céljából.
- Összevetés (használat) – a tárolt és a felhasználáskor készülő biometrikus adatok vagy biometrikus sablonok összevetése.
- Az összevetést végző egység a rendszer kezelője által előre beállított egyezőségi mérték (általában az adattárolóban rögzített és a helyben mért paraméterek egyezésének százaléka) alapján szolgáltat eredményt a személyazonosság megállapításáról (vagy az elutasításáról).

biometrián alapuló személyazonosító rendszerek pontossága

fenti személyazonosító rendszerek akkurátus működését általában három értékkel szokták llemezni.[1]

téves visszautasítási arány *(False Rejection Rate, **FRR**)* annak a valószínűségének mértéke, ogy egy biometrikus rendszer hibásan elutasítja egy jogosult felhasználó pl. belépési szándékát. Az ányszám megmutatja, hogy hány téves visszautasítási esemény történik adott számú belépési eményre vonatkoztatva. A gyakorlatban az FRR értékek – a mért biometrikus jellemző ggvényében – tipikusan 1 ‰ (ezrelék) és 6‰ között mozognak.

téves elfogadási arány *(False Acceptance Rate, **FAR**)* annak a valószínűségének mértéke, hogy y biometrikus rendszer hibásan elfogadja egy jogosulatlan felhasználó belépési szándékát. Az ányszám megmutatja, hogy hány téves elfogadási esemény történik adott számú belépési eményre vonatkoztatva. A gyakorlatban a FAR értékek – a mért biometrikus jellemző ggvényében – tipikusan 0,001 és 2 ‰ (ezrelék) között mozognak (vagyis jellemzően agyságrendekkel kisebb a téves elfogadások aránya a téves visszautasításokénál).

z **egyenlő hibaarány** *(Equal Error Rate, **EER**)* az az összehasonlítási küszöbérték, ahol az FRR s a FAR értékek megegyeznek. Az EER segítségével egyszerűen összehasonlíthatóak a különböző iometrikus azonosító rendszerek pontossága: az alacsonyabb EER értékű rendszer a pontosabb.

fenti adatok tájékoztató jellegűek, mert ezen értékeket több tényező is jelentősen befolyásolhatja.

[1] SYRIS Technology Corp.: About FAR, FRR and EER (2004) Version 1.0

Válaszok a feltett kérdésekre:

Informatikai szempontból mennyiben igazolható a Sporttv.-nek az a rendelkezése, hogy a biometrikus adatból képzett HASH-kód „vissza nem fejthető, titkosított, algoritmizált alfanumerikus kód"?

A T/156. számú törvényjavaslat eredeti normaszövegében szereplő „HASH-kód" kifejezés értelmetlen. A 2004. évi I. törvény 72/A. § (2) bekezdése **nem nevesíti a biometrikus sablont előállító eljárást,** de **ellentmondásosan írja elő a biometrikus sablon előállításának módját,** illetve **szükségtelenül szabályozza annak megjelenítési formáját.**

A „vissza nem fejthető" kitétel logikailag ellentmond a „kód" kitételnek, az „alfanumerikus" kitétel pedig szükségtelenül vagy szakszerűtlenül szabályozza az előállított adatok formai megjelenítését. A „titkosított" kitétel egyáltalán nem szerepel a hatályos jogszabályban.

Amennyiben a jogalkotó szándéka egy egyirányú, veszteséges adatleképezési eljárás alkalmazásának előírása volt, amely eljárás során biztosítani kívánta a biometrikus sablon illetéktelenek által való megismerése elleni védelmet, akkor ezt nem sikerült szabatosan megfogalmazni.

A **biometrikus sablonnal szemben támasztott** – a felhasználás céljából fakadó – jogi és technikai **követelmények** a következőek lehetnek:

- a biometrikus adatból egyirányú, veszteséges, vissza nem fejthető leképezéssel előállított,
- kizárólag a biometrikus sablonok összehasonlítására alkalmas jellemzőket tartalmazó,
- előállítás után utólag titkosítással védendő adatok összessége.

A jelenleg hatályos jogszabály szükségtelenül korlátozza a biometrikus rendszerek működési elvét, mert mindenképpen biometrikus sablon alkalmazását írja elő, holott a biometrikus sablon előállítása adatvédelmi szempontból szükségtelen lépés, azonban a gyakorlati működés szempontjából – a rögzített biometrikus jellemző függvényében – nem minden esetben szükséges vagy célravezető a biometrikus sablon alkalmazása. A jogszabály továbbá explicit módon nem írja elő a biometrikus adat vagy sablon bizalmassága biztosításának kötelezettségét.

Milyen HASH kódolási technikák ismertek? Ezek közül melyek a legelterjedtebb kódolások? E kódolási technikák milyen adatvédelmi-biztonsági kockázatokat hordoznak magukban?

Az előzőekben leírtak ismeretében továbbra is kijelenthető, hogy a biometrikus sablont előállító hasítóeljárások nem kódolási eljárások. A biometrikus adatokat transzformáló számítógépes algoritmusok döntő többségében szabadalmaztatott eljárások, ezért a biometrikus azonosítást biztosító rendszerek gyártónként eltérő, egyedi sablon formátumokat alkalmaznak.

Az alkalmazott hasítóeljárások a mért biometrikus jellemzőtől is függenek, ezért azonos gyártó esetén is különböző transzformációkat alkalmaznak a különböző biometrikus jellemzők leképezésére (mivel pl. egy ujjnyom és egy íriszkép jellemzőinek leképezési eljárása teljesen más).

A nyílt forrásokból elérhető irodalom[2] az alábbi táblázatban foglal össze néhány ismert transzformációs eljárást.

A hasító eljárás neve	**A mért biometrikus jellemző**	**A leképezés alapja**	**A transzformáció módja**	**A biometrikus sablon megjelenési formája**
Biohashing, PalmHash	arc, tenyérlenyomat, ujjlenyomat	vektorok (Fisher-féle megkülönböztető jellegek)	véletlenszerű mátrix-szorzás	vektor
BioPhasor	ujjlenyomat	vektorok (FingerCode)	nem-lináris	vektor
Cancelable Face	arc	vektorok (arckép)	véletlenszerű mátrix-konvolúció	vektor
Robust Hash	arc	vektorok (arckép mátrix egyes értékei)	multimodális függvény optimalizálás	vektor
Class Distribution Preserving Transformation	arc	vektorok (FisherFace jellegek)	jellemzővektor és adott ponthalmaz távolságának mérése	vektor
Cancelable Iris	írisz	vektorok (Log-Gabor reakció)	körkörös eltolódás és kombináció	vektor
Histogram of minutiae trangles	ujjlenyomat	pontok (barázdák elágazása és végződése)	minúcia háromszög jellegek hisztogramjának hasítása	vektor
Symmetric Hash	ujjlenyomat	pontok (minúciák komplex számokként)	minúciák sorrendre érzéketlen függvényeinek sorozata	minúciatérkép
Cancelable Fingerprints	ujjlenyomat	pontok (minúciatérkép)	képtömörítés	minúciatérkép
Alignment free cancelable fingerprint	ujjlenyomat	pontok (minúciatérkép orientációval)	minúciák leképezése a környezetük orientációja alapján	minúciatérkép
Cuboid based Minutiae Aggregates	ujjlenyomat	pontok (minúciatérkép)	minúcia jellemzők egyesített kiválasztása véletlenszerű helyi régiókból	vektor

[2] http://www.cse.msu.edu/biometrics/Publications/SecureBiometrics/NagarTempTransSecAnalysis_SPIE10.pdf

A biometrikus sablonok előállításának célja alapvetően nem az adatok titkosítása, hanem az adatok egyszerűsítése, ezért az adatvédelmi-biztonsági kockázatok elsősorban az illetéktelen megismerhetőségben rejlenek, ezért szükséges a sablon adattartalmát titkosítással védeni.

A sablon előállítási módjának egyetlen, a rendszer megbízható működésére kiható kockázata, hogy amennyiben a hasító eljárás túlságosan absztrahálja a biometrikus adatot, akkor annyira absztrakt biometrikus sablon keletkezhet, amely túlságosan sok egyezőséget mutathat más – egyébként eltérő – biometrikus adatokból képezett biometrikus sablonokkal. Ez esetben a biometrikus azonosító rendszer alkalmazása során a téves elfogadások száma jelentősen megnövekedhet.

A fenti táblázatban felsorolt biometrikus hasítóeljárások biztonsági kockázatainak részletes elemzését a 2. számú lábjegyzetben hivatkozott tudományos publikáció tartalmazza.

A Sporttv. rendelkezése alapján eddig kiépített biometrikus azonosítási rendszerek pontosan milyen kódolási technikát alkalmaznak? Ezeknek milyen adatvédelmi-biztonsági kockázatai vannak?

A Sporttv. nem nevesíti a biometrikus sablon készítéséhez alkalmazandó technikai eljárásokat, (ugyanakkor a „biometrikus adat" taxatív felsorolásával elzárja más biometrikus jellemzők felhasználása elől a lehetőséget) valamint **a jogszabály szakszerűtlen szövegezése miatt nem egyértelmű**, hogy kódolás alatt a biometrikus adat biometrikus sablonná való leképezését érti, vagy az elkészült biometrikus sablon adattartalmának titkosítását.

Kizárólag a jogszabályban rögzítettek alapján ezért nem állapítható meg, hogy pontosan milyen leképezést és/vagy titkosítást alkalmaznak a törvénynek megfelelő biometrikus rendszerek.

Az amicus curiae-ben leírt rendszeren kívül nincs tudomásunk – a Sporttv. alapján kiépített – biometrikus azonosítási rendszert használó sportlétesítményről. Az amicus curiae sem tartalmazza az általuk használt rendszer vonatkozásában a biometrikus adatokon végzett transzformáció nevesítését, illetve a keletkező biometrikus sablon adatainak titkosításához használt rejtjelezési eljárás pontos leírását. Ezen adatokat vélhetően a szóban forgó biometrikus azonosítórendszer műszaki dokumentációjából lehet csak megismerni.

A fenti adatok hiányában az adatvédelmi-biztonsági kockázatokat illetően ugyanazok a megállapítások érvényesek, amelyek a 2. kérdésre adott válaszban is megfogalmazásra kerültek.

A fentiekben hivatkozott amicus curiaeben megjelölt, ún. AES kódolás a legbiztonságosabb kódolásnak tekinthető? E kódolás valóban olyan biztonsági szintű, mint ahogy erre az amicus curiae beadványban hivatkoztak?

Az *Advanced Encryption Standard (AES)* egy elektronikus adatok titkosítására alkalmas eljárás specifikációja. **Az AES nem kódolás, hanem egy blokkrejtjelező titkosítási eljárást leíró szabvány.** Az AES kriptográfia önmagában csak egy eljárást jelöl, de nem pontosítja a megvalósítás módját.

Hasonlattal élve: biztonságos-e a PIN (személyes azonosítószám)? Nyilván nem mindegy, hogy egy 4 jegyű, vagy egy 16 jegyű PIN-t kell kitalálni. Előbbinél mindössze 10.000 (tízezer) próbálkozásból kitalálható a kulcs, míg az utóbbi esetében 10.000.000.000.000.000 (tízbilliárd vagy tízezerbillió) számkombinációt kell végigpróbálgatni.

Az AES kriptográfiai szabvány 128 bit méretű bemeneti adatblokkokat definiál, de három választható kulcsmérete is ismert: 128, 192 és 256 bites. A nagyobb kulcsméret több kombinációt tesz lehetővé, vagyis több a lehetséges rejtjelkulcsok száma – ezáltal nehezebben kitalálható, vagyis nagyobb biztonságot nyújt. Ebből a szempontból tehát az AES-256 titkosítás biztonságosabbnak tekinthető, mint az AES-128 titkosítás.

Az amicus curiae dokumentumban azonban **nem nevesítik a biometrikus azonosító rendszerükben alkalmazott konkrét AES megvalósítás kulcsméretét**.

Egy titkosítást azonban nem csak a titkosító kulcs valamennyi kombinációjának végigpróbálgatásával, hanem a titkosító eljárás sérülékenységének ismeretében is fel lehet törni. A PIN hasonlatához visszatérve, hiába 16 jegyű egy aktatáskán a számkombinációs zár, ha a zárszerkezet tárcsái a titkosító kulcsnak megfelelő számjegyéhez való tekerésekor kattanó hangot adnak. Ennek ismeretében ugyanis már néhány próbálkozás után kitalálható a helyes kulcs.

Az AES titkosító eljárás ún. helyettesítő-permutáló hálózatot (*substitution-permutation network, SPN*) használ az adatblokkok titkosítására. Szabványos 128 bites bemeneti blokkok esetében az AES 4x4-es mátrixokat használ a titkosítás során. A kulcsméret meghatározza, hogy a bemeneti információt hány átalakítási ciklus éri, míg eléri a végleges, titkosított állapotát. Minden ciklus számos lépést foglal magába, ezek között van az a lépés is, ami kulcs alapján módosítja a mátrixot. A visszaalakítás során ugyanennyi ellentétes ciklust hajtanak végre a kulcs segítségével.

Az AES titkosító eljárás biztonsági megítélésére jellemző, hogy 2003. júniusában az Egyesült Államok kormánya is bejelentette, hogy az AES használható a minősített adatok védelme érdekében is: "Az AES szerkezete és erőssége minden kulcshossz mellett (128, 192 és 256 bites kulcsokkal) megfelelő a minősített adat védelméhez, a "TITKOS!" minősítésig. A "SZIGORÚAN TITKOS!" minősítésű adathoz 192 vagy 256 bites kulcshosszra van szükség."[3]

A biometrikus sablonok AES-256 rejtjelezés útján való titkosítása ésszerűen elegendő védelmet biztosíthat az adatok bizalmasságának megőrzésére az elkövetkezendő évtizedekre.

---

[3] http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf

Milyen informatikai biztonsági kockázatai vannak egy biometrikus azonosítási rendszer működésének? Milyen kockázatokat rejt magában a biometrikus sablon előállítása és tárolása?

A biometrikus sablon előállításával és tárolásával összefüggő kockázatok:

- a biometrikus adat felvételezése rossz minőségben történik meg, ezért a FAR és FRR értéke megnövekedik;
- a nyers biometrikus adat sablonná történő transzformálása nem megfelelő algoritmussal történik meg, ezért a FAR és FRR értéke megnövekedik;
- a biometrikus sablon elkészítése után a felvételezett biometrikus adat nem kerül **helyreállíthatatlanul** törlésre;

Biztonságosabb adattárolást eredményez-e a biometrikus sablonok központi adatbázisban való tárolása, mint például egy, az érintett személy birtokában lévő chipkártyán való nyilvántartás?

A biometrikus sablonok fizikai tárolásának módja nem kizárólag biztonsági vonatkozású kérdés, hanem már az adatokkal való rendelkezés jogi kérdéseit is feszegeti.

A központi adatbázisban való tárolás esetében az adathoz való illetékes hozzáférhetőség szabályozását – vagyis az adat fizikai, adminisztratív és informatikai védelmét – egy biztonsági szakemberekkel rendelkező szervezet valószínű, hogy hatékonyabban tudja megoldani, mint egy képzetlen magánszemély.

Ugyanakkor az adatbázist üzemeltető informatikai rendszer kompromittálódása esetén minden ott tárolt információt egyszerre megszerezhet, manipulálhat az elkövető. Valamennyi klubkártya tulajdonos teljes mértékben a szervező informatikai rendszerének biztonságára hagyatkozik a személyükhez köthető, azonosításukra alkalmas biometrikus sablonjaik kezelését és védelmét illetően.

Ezzel szemben a chipkártyán tárolt adat akkor válhat támadás áldozatává, ha a chipkártya kikerül a klubkártya tulajdonos birtokából (akár szándékosan, akár gondatlanul). Ez esetben azonban az elkövető csak egyetlen klubkártya (személy) titkosított biometrikus adatához vagy sablonjához juthat hozzá.

A chipkártyán tárolt adat ezért a teljes rendszer biztonsága, valamint a klubkártya tulajdonosok személyhez köthető adatok felett való rendelkezési joga szempontjából is előnyösebb lehet.

A beléptetés biztonságát illetően nem a adatok tárolásának helye (adatbázis vagy chipkártya), hanem az adatok összevetésének módja a mérvadó. Adatbázis alkalmazása esetén a beléptetéskor mért biometrikus adatot az adatbázisban szereplő előzetesen rögzített biometrikus adattal (vagy adatokkal) kell összehasonlítani. Megvalósítástól függően a mért adat és a rögzített adat összevetése történhet egy-az-egyben *(1:1)*, vagy a mért adat az adatbázisban szereplő valamennyi adattal kerül összevetésre *(1:n)*.

Az adatbázisban tárolt biometrikus adatok nagy mennyisége és mérete teszi szükségessé és célszerűvé a biometrikus adatok helyett a biometrikus sablonok alkalmazását. Belátható, hogy *1:n* arányú összevetés esetében jelentősen megnöveli a téves elfogadás esélyét egyetlen minta összevetése több ezer másik mintával (adatbázisban tárolt minták), a minták egy-az-egyben való összevetéséhez képest (adatbázisban vagy chipkártyán tárolt minta).

Következésképpen ilyen megvalósítás esetén a téves elfogadások valószínűsége az összevetett minták számával (*n* értékével) arányosan nő. A chipkártyán tárolt adat esetében a beléptetéskor mért adatot csak a chipkártyán tárolt egyetlen mintával kell összehasonlítani, vagyis kizárólag *1:1* arányú összevetés történhet.

Mennyire megbízható egy biometrikus azonosítási rendszer működése? Előfordulhat-e, hogy az automatikus azonosítási rendszer ugyanabból a beviteli adatból (pl. egy ujjnyomat) eltérő kódot állít elő, és ebből következően akár az azonosítási, akár az ellenőrzési folyamat nem pontos?

A biometrikus azonosítási rendszerek két különböző időpontban, általában eltérő körülmények között végrehajtott mérés eredményeit vetik össze. A mérési eredmények szórása miatt, előfordul, hogy tévesen azonosítja a biometrikus jellemzőt, illetve tévesen utasítja el az azonosítását a biometrikus jellemzőnek.

A bevezetőben meghatároztuk a biometrikus rendszerek pontosságát jellemző összehasonlító értékeket. Ezek a téves elfogadási ráta (FAR) és a téves visszautasítási ráta (FRR). A megadott értékek tájékoztató jellegűek, ugyanis nagyon nagy mértékben múlik a biometrikus azonosítás például az adatfelvételezéskor rögzített nyers biometrikus adatok minőségén, a sablon készítéshez használt algoritmus megfelelőségén. Egy rossz minőségben felvett kezdeti adat egy nem megfelelően akkurátus sablonkészítő algoritmussal akár 50% FAR és FRR értékeket is produkálhat.

Mivel a biometrikus adat beolvasása szórást mutat, ezért beolvasásonként hasonló, de mindig eltérő adat fog előállni. Az azonosítás a biometrikus sablonok egyezőségi mértékén alapul, és a beállított küszöbértéktől függ. Ujjlenyomat esetén általában minimum 10-12 azonosítási pont egyezését követelik meg. Az egyezőségi mérték küszöbszintje változtatásának következményei:

- minél magasabb az egyezőségi mérték küszöbszintje, annál magasabb a téves elutasítás aránya és az abból származó frusztráció és késedelem (a beléptetés során a helyszínen valószínűleg többször is be kell olvasni a biometrikus adatot az elfogadáshoz);
- minél alacsonyabb, annál magasabb a téves elfogadás aránya és az abból származó biztonsági kockázat (a nem egyező, de elegendően hasonló biometrikus adat téves elfogadása).

A megoldás csak kompromisszummal lehetséges, vagyis a megbízható és a gördülékeny azonosítást lehetővé tévő, elfogadható FAR/FRR értékeket eredményező sablonképzési algoritmust, illetve összehasonlítási küszöbértéket kell alkalmazni. Megjegyzendő, hogy az összehasonlítási küszöbértéket a rendszer kezelője állíthatja be, eképpen is befolyásolva a rendszer biztonságát.

Informatikai szempontból milyen egyéb adatbiztonsági kockázatai vannak egy biometrikus azonosítási rendszer működésének?

Egy biometrikus azonosítórendszer adatbiztonsági kockázatai – bármely más informatikai rendszerhez hasonlóan – nagymértékben függenek a technikai megvalósítás módjától (az alkalmazott hardverek és szoftverek összességétől), az informatikai rendszernek otthont adó objektum fizikai védelmétől, a rendszer működtetése során alkalmazott adminisztratív védelmi szabályrendszertől, a felhasználók és az üzemeltetők védelmi tudatossági szintjétől, valamint számos egyéb tényezőtől.

Egy adott rendszer adatbiztonságának valódi mértékét a rendszerre (és felhasználóira) irányuló specifikus biztonsági audit keretében történő sérülékenység-vizsgálat és kockázatelemzés segítségével lehet tényszerűen felmérni. A Sporttv. a szervező informatikai rendszerének biztonsági követelményeire vonatkozó előírásokat nem tartalmaz. A 2013. évi L. törvény pedig csak az állami és önkormányzati szervek elektronikus információbiztonsága kapcsán rendelkezik a fenti elemzések végrehajtásáról.

dapest, 2016. május 04.

[redacted]
iü. informatikai szakértő

[redacted]
iü. okmányszakértő

tta:

[redacted]