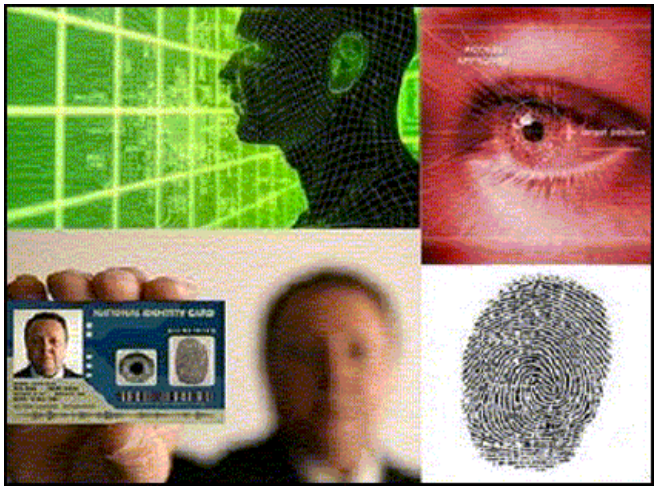
Biometria

„Biometrikus” alatt olyan rendszereket értünk, amelyek vagy személyek mérhető fizikai jellemzőit – az ujjlenyomatot, a DNS-t, a retina véredény-struktúráját, az arcvonásokat, esetleg a test szagát – használják, vagy egyedi viselkedési jellegzetességeket vizsgálnak, mint mondjuk a testtartás, a hang, esetleg a billentyűleütési szokások. E rendszerek célja, hogy megállapítsák, ellenőrizzék a személyazonosságot, vagy kategorizálják az egyéneket.



Egyes országokban felveszik az állampolgárok ujjlenyomatait vagy más biometrikus azonosító adatait, és ezeket a személyazonosító igazolványokon vagy egy adatbázisban tárolják. Első lépésként tehát rögzítik az adott személy jellemzőit, majd egy biometrián alapuló rendszerben tárolják. A későbbiekben aztán ezt az eredeti biometrikus információt veszik elő és használják arra, hogy azonosítsák a szóban forgó személyt. A számítástechnikai kapacitás fejlődése azt eredményezte, hogy mára léteznek automatikus biometrikus rendszerek, amelyek például egész tömegek másodpercek alatti azonosítását is lehetővé teszik.

1.1 Milyen céllal fejlesztették ki az első biometrikus azonosítórendszereket?

A 19. században az államok igazságügyi rendszereinek fejlődése szükségessé tette egy központosított, formalizált személyazonosítási módszer bevezetését. A jogrendek többsége a törvénnyel először összeütközőkkel elnézőbb volt, mint a visszaeső bűnözőkkel szemben. Ezért is volt szükség olyan formalizált nyilvántartásra, amelyben az elkövetett bűncselekményeket és az elkövetők valamilyen egyedi jellemzőit rögzítették. Franciaországban Alphonse Bertillon dolgozta ki a „Bertillonage”-nak nevezett eljárást, amely az egyének részletesen rögzített testi jellemzőit, például magasságukat, karjuk hosszát, külsejük leírását, illetve fotókat használt személyazonosításra. Az 1890-es években aztán egy újabb, jobb eredményekkel kecsegtető rendszer született, miután Francis Galton kidolgozott egy módszert a bűnözők azonosítására ujjlenyomatuk alapján, amely sokkal egyedibb jellemzőnek bizonyult, mint a Bertillon használta adatok. A 20. században aztán újabb, a személyazonosításra alkalmas jellemzőket fedeztek fel. Frank Burch 1936-ban állt elő az ötlettel, hogy a retina mintázata pontos azonosítóként szolgálhatna, az 1960-as években pedig létrejöttek az arc- illetve hangfelismerést lehetővé tévő technológiák.

1.2 Mire használják a biometrikus rendszereket?

A biometrikus azonosítást hagyományosan a rendvédelmi szervek használják bűncselekmények ismert vagy még ismeretlen elkövetőinek azonosítására, illetve annak megállapítására, hogy valaki jogosult-e belépni egy védett területre, például kormányhivatalokba, kutatólaborokba stb.

A 21. században a biometriát egyre elterjedtebben használják a határvédelem területén. Egyes országokban a vízumért folyamodók egyes biometrikus jellemzőit is rögzítik. Az országba belépéskor aztán ezeket az adatokat például arra használják, hogy megállapítsák, az illető személy belépését korábban már megtagadták, esetleg biztonsági kockázatot jelent, vagy előzőleg már a megengedett időnél tovább tartózkodott az országban. Az Európai Unióban például tíz ujjlenyomatot és egy digitális fotót rögzítenek azokról, akik EU-s vízumért folyamodnak. Ezeket az adatokat a VIS-adatbázisban (Visa Information System – Vízuminformációs Rendszer) tárolják. Az EU létrehozta a hasonlóan működő EUROADAC adatbázist is, amelyben a menedékjog-

okért folyamodók, illetve az EU területén felfedezett olyan bevándorlók adatait rögzítik, akik ellenőrzés nélkül jutottak át a határokon. Az adatbázis segít a menedékkérők és illegális bevándorlók kezelésének metódusát rögzítő, 2003-ban elfogadott dublini rendelet hatékony végrehajtásában.

A biometria katonai alkalmazási területei között megemlíthetjük, hogy az USA fegyveres erőinél hordozható készülékeket rendszeresítettek, amelyek az afganisztáni és iraki hadszíntereken lehetővé teszik, hogy rutinszerűen rögzítsék a katonákkal kapcsolatba kerülő személyek szivárványhártya-mintázatát vagy más biometrikus azonosítóit. A gyanúsnak nyilvánított embereket aztán felveszik az „Engedélyezett Biometrikus Megfigyelési Listára", amely lehetővé teszi a terepen szolgáló katonák számára, hogy azonosítsák a terroristagyanús egyéneket, vagy felfedezzék például, ha valaki ismert gerillacsoportokkal áll kapcsolatban, és emiatt nem alkalmazható az amerikai hadsereg által fenntartott külföldi létesítményekben. A legutóbbi információk szerint a listán 209 ezer, a világ minden tájáról származó személy adatai szerepelnek.

Igaz, hogy a biometrikus azonosítási eljárásokat a 20. század elejétől eredetileg biztonsági célokra hozták létre és fejlesztették, közben azonban egyre inkább magáncégek is alkalmazták őket. Előnyük elsősorban abban rejlik, hogy a jelszavakkal, kulcsokkal vagy beléptetőkártyákkal ellentétben a személyes jellemzőket igencsak nehéz elfelejteni vagy elveszteni. Ezért aztán sokan biztonságosabbnak és nehezebben kijátszhatónak tartják ezeket, mint a hagyományos megoldásokat. Az utóbbi években számos területen terjednek robbanásszerűen a biometrikus azonosító módszerek, például egyre több csúcskategóriás okostelefonba építenek ujjlenyomat-olvasót. A Facebook arcfelismerő szoftvert használ, hogy a felhasználók feltöltött fényképein automatikusan javaslatot tegyen a felvételen szereplők azonosítására. A cég DeepFace nevű, tesztelés alatt álló projektje állító-

Hogyan működik a biometrikus azonosítás?

Az első lépés az illető személy biometrikus adatának, például ujjlenyomatának vagy szivárványhártya-mintázatának rögzítése, általában egy kép formájában. Az információt képként, vagy egy, a biometrikus adatokból egy algoritmus segítségével létrehozott sablon formájában tárolják. A magánszféra védelmének érdekében a javasolt eljárás az, hogy csak a sablont őrzik meg, a képet pedig nyom nélkül törlik.

A biometrikus adat – akár a képről, akár a sablonról van szó – számos helyen tárolható, például a rögzítést végző központban – mondjuk a felvételt végző szerkezetben – várhatja a további felhasználást, vagy a személy által magánál hordott intelligens eszközön, például egy chippel ellátott személyazonosító kártyán. Az is elképzelhető, hogy elküldik egy központi adatbázisba, és ott tárolják el, ahol aztán több rendszer is hozzáférhet az adatokhoz.

Ha a biometrikus alapú „összevetés" sikerrel jár, akkor a rendszer felismeri az adott személyt. Amennyiben sikertelen az összevetés, akkor a személy ismeretlennek számít, és a rendszer „visszautasítja". Az első rögzítéskor készített kép vagy sablon ritkán egyezik meg teljesen az azonosítás pillanatában felvett biometrikus jellemzővel. Az ilyen jellemzők ugyanis hajlamosak kis mértékben megváltozni, de a felvétel körülményei, vagy a használt berendezés is változhat. Elkerülhetetlen, hogy az azonosítás bizonyos hibaszázalékkal működjön.

A biometrikus rendszerek felhasználhatók bűnmegelőzési célokra is, különösen, ha a vizsgált személyek viselkedési jegyeinek vizsgálatának elemzésére használják őket, és a cél nem az azonosítás, hanem a megfigyelt emberek kategóriákba sorolása. Az intelligens megfigyelő kamerákba épített arcfelismerő és viselkedéselemző funkciók tulajdonképpen a térfigyelő kamerák biometrikus képességekkel történő kiegészítéseként működnek.

lag 97,25 százalékos pontossággal megállapítja, hogy két képen ugyanaz a személy látható-e. A bankok megbízható hangazonosító rendszereket fejlesztenek, hogy az ügyfelek pusztán egy jelszó bemondásával a telefonon át elérhessék bankszámlájukat vagy jóváhagyják tranzakcióikat. Számos vállalatnál használnak ujjlenyomat-olvasókkal felszerelt céges laptopokat, így elméletileg elzárva az illetéktelen személyeket a bizalmas információkhoz való hozzáféréstől. Egyes köztéri reklámfelületek más és más hirdetést mutatnak attól függően, milyen nemű vagy korú személy áll előttük.

A biometriás rendszereket azonban az azonosításon túl egyre inkább viselkedéselemzésre is használják. Számos edzést segítő eszköz és alkalmazás használ valós idejű biometrikus adatokat, például a pulzus- vagy a légzésszámot, hogy személyre szabott tanácsokkal vagy feladatokkal lássa el a felhasználókat. Biztonsági területen pedig a biometrikus adatokkal dolgozó eszközöket meglévő rendszerekbe építik be (például a köztéri kamerák arcfelismerő képességgel történő felvértezése), ez pedig új távlatokat nyit a felügyeletben és megfigyelésben. Ebben az összefüggésben fontos megjegyezni, hogy az ilyen fejlett rendszerek távolról vagy mozgás közben, az alany tudta nélkül is képesek információkat gyűjteni. Adott esetben a rendszer például riasztást adhat le, ha mondjuk egy köztéri kamera a rendőrségi adatbázisban szereplő ismert bűnözőt azonosít.

1.3 Milyen előnyökkel jár?

A biometriás rendszerek a következő módokon javíthatják a közbiztonságot:

- A biometrikus adatokon alapuló azonosítókat immár több mint egy évszázada használják a rendvédelmi szervezetek ellenőrzésre és azonosításra. Az arcvonásokat rögzítő, vagy a DNS-t elemző rendszerek igen hatékonyan segíthetnek a bűnüldözésben és súlyos bűncselekmények elkövetőinek azonosításában.
- Az összegyűjtött biometrikus információk arra is használhatók, hogy növeljék a bizalmas adatok feldolgozásának biztonságát. Például segíthetnek abban, hogy mondjuk egy telefonszolgáltató cégnél kizárólag az arra felhatalmazott emberek férjenek hozzá a kötelezően megőrzött helymeghatározási adatokhoz.

1.4 Milyen problémákat vet fel?

Több negatívum is van, amiket figyelembe kell venni:

1. A biometria nem tévedhetetlen.
   - Kimondható, hogy egy biometrikus jellemzőről készült két digitális „felvétel” soha nem lesz pontosan ugyanolyan. A használt felszerelés eltérése, vagy az olyan környezeti körülmények, mint mondjuk a hőmérséklet vagy a megvilágítás különbsége, téves igazolásokhoz és téves visszautasításokhoz vezethet. Bármely biometrikus rendszer bizonyos százalékban tévesen azonosíthat egy személyt, és hozzáférést engedélyezhet nem megfelelő embereknek, más esetekben pedig arra az eredményre juthat, hogy a jogosult személyek adatai nem egyeznek meg saját, korábban felvett biometrikus azonosítójukkal.
   - Ráadásul az emberek biometrikus jellemzői megváltozhatnak életük során, például a korral, esetleg egy műtét vagy egy baleset következményeként. Előfordulhat, hogy a biometrikus rendszerek ilyen esetben többé nem „ismerik fel” őket.
   - A biometrikus adatokat is meg lehet hamisítani, ez pedig fokozza a személyiségtolvajlás veszélyét.
   - A technológia mai szintje mellett még mindig túl könnyű átverni például egy arcfelismerő rendszert a megjelenés olyan egyszerű megváltoztatásával, mint a más hajviselet, arcszőrzet, smink, szemüveg vagy kontaktlencse viselése, stb.

2. A múltban a biometrikus azonosítás drága és időigényes volt. Ez korlátozta azt a hatást, amelyet az ilyen technológiák az emberek személyes adatainak védelméhez fűződő jogaira gyakoroltak. Mára ez megváltozott, ami például genetikai alapú diszkriminációhoz, illetve a magánszféra fokozatos leépüléséhez vezethet, ha nincsenek megfelelő biztosítékok. Például a megfigyelő rendszerek és az okostelefonok felszerelése a közösségi hálózatok adatbázisából építkező arcfelismerőkkel az egyének anonimitásának és szabad, ellenőrizetlen mozgásának a végét jelenthetik.
3. A legtöbb esetben a biometrikus adatok felvételéhez szükség van az adott személy együttműködésére. Ilyen például az ujjlenyomatok rögzítése, ahol az egyénnek lehetősége van hozzájárulást adni adatai rögzítéséhez, illetve meggyőződni azok biztonságos kezeléséről. Adatok felvétele lehetséges azonban a célszemélyek tudta és beleegyezése nélkül is, például egy arcfelismerővel felszerelt kamera felhasználásával. Ez súlyosan befolyásolja az egyének önkéntes beleegyezéshez fűződő jogait, vagy azt, hogy megtudják, pontosan ki és mire használja adataikat.
4. Ha a biometrikus jellemzőket úgy tekintjük, mintha megváltoztathatatlanok lennének, kellemetlen meglepetést okozhat, ha már a felvételnél hiba vagy nem kívánt beavatkozás történik, amely a személy téves megbélyegzéséhez vezethet.

IMPRESSZUM

*Ez a tájékoztató a **SurPRISE** (**Sur**veillance **PRI**vacy and **SE**curty) európai kutatási projekt keretében készült, amelyben a Medián Közvélemény- és Piackutató Intézet is részt vett, és amelyet az Európai Unió Kutatási és Technológiafejlesztési Hetedik Keretprogramja támogatott. A 2015 januárjában lezárult SurPRISE project fő célkitűzése az volt, hogy összegyűjtse az európai polgárok véleményét az új biztonsági technológiákról.*

További részletes információk a projektről a Medián honlapján (www.median.hu) és a kutatás nemzetközi honlapján találhatók: http://surprise-project.eu/

Szerzők: Matthias Vermeulen (European University Institution) and Szénay Márta (Medián)

Design: Bartha Zsolt (Medián)

Illusztráció: © KIVI NIRIA DV, 2011

Medián, 2015. január