A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT

00720/12/HU

WP193

3/2012. sz. vélemény a biometrikus technológiák terén történt fejleményekről

Elfogadás időpontja: 2012. április 27.

Ez a munkacsoport a 95/46/EK irányelv 29. cikke alapján jött létre. A munkacsoport adatvédelemmel, valamint a magánélet védelmével kapcsolatos kérdésekkel foglalkozó független európai tanácsadó szerv. Feladatait a 95/46/EK irányelv 30. cikke és a 2002/58/EK irányelv 15. cikke határozza meg.

A titkársági feladatokat ellátja: Európai Bizottság, Jogérvényesülési Főigazgatóság, C. Igazgatóság (Alapvető jogok és uniós polgárság), B-1049 Brüsszel, Belgium, MO-59 06/036. sz. iroda.

Honlap: http://ec.europa.eu/justice/data-protection/index_en.htm.

Összefoglalás

A biometrikus rendszerek szorosan kapcsolódnak egy adott személyhez, mivel az egyén bizonyos egyedi tulajdonságát használják fel az azonosításhoz, illetve a hitelesítéshez. Míg a személyek biometrikus adatai törölhetők vagy módosíthatók, a forrást, amelyből az adatokat kinyerték, általában sem módosítani, sem törölni nem lehet.

A biometrikus adatokat sikeresen és hatékonyan használják a tudományos kutatásban, kulcsfontosságú szerepet töltenek be az igazságügyi szakértői munkában, és értékes elemei a hozzáférés-ellenőrzési rendszereknek. Segíthetnek a biztonság szintjének növelésében, és könnyűvé, gyorssá és kényelmessé tehetik az azonosítási és hitelesítési eljárásokat. Korábban költséges volt e technológia használata, és e gazdasági korlát miatt csak mérsékelt hatással volt az egyének adatvédelmi jogaira. Az elmúlt években ez drasztikusan megváltozott. A DNS-elemzés gyorsabbá vált, és már szinte mindenki számára megfizethető. A technológiai fejlődés miatt olcsóvá váltak a tárhelyek és a számítógépes teljesítmény, ami lehetővé tette, hogy fényképek milliárdjait tartalmazó online képalbumok és közösségi hálózatok jöjjenek létre. Az ujjlenyomat-olvasók és a videomegfigyelési eszközök olcsó műszaki cikké váltak. E technológiák fejlődése hozzájárult ahhoz, hogy sok művelet kényelmesebb legyen, elősegítette sok bűncselekmény megoldását, és megbízhatóbbá tette a hozzáférés-ellenőrzési rendszereket, azonban alapvető jogokat érintő új fenyegetések kialakulásához is hozzájárult. A genetikai diszkrimináció valódi problémává vált. A személyazonosság-lopás már nem csak elméletben jelent fenyegetést.

Míg a nagy populációkra kiterjeszthető és a közelmúltban adatvédelmi aggályokat felvető egyéb új technológiák nem feltétlenül összpontosítanak arra, hogy egy meghatározott egyénnel kapcsolatban hozzanak létre közvetlen kapcsolatot – illetve egy ilyen kapcsolat létrehozása jelentős erőfeszítéseket igényel –, a biometrikus adatok éppen a jellegükből adódóan közvetlenül kapcsolódnak az egyénekhez. Ez nem mindig előny, hanem inkább számos hátránya lehet. Ha például a videomegfigyelési rendszereket és okostelefonokat a közösségi hálózatok adatbázisán alapuló arcfelismerő rendszerekkel látják el, az véget vethet az anonimitásnak és az egyének nyomon követés nélküli mozgásának. Az ujjlenyomat-olvasók, az érmintázat-olvasók, illetve a kamerába mosolygás mindazonáltal felválthatják a kártyákat, a kódokat, a jelszavakat és az aláírásokat.

Ez a vélemény ezekkel és más közelmúltbeli fejleményekkel foglalkozik, hogy felhívja mind az érintett személyek, mind a jogalkotó szervek figyelmét a problémára. Ezek, a nagyon gyakran csak a felhasználói élmény javítását és az alkalmazások kényelmesebbé tételét szolgáló technológiaként bemutatott technikai újítások megfelelő biztosítékok bevezetése hiányában a magánélet fokozatos megszűnéséhez vezethetnek. Ezért ez a vélemény olyan technikai és szervezeti intézkedéseket határoz meg, amelyek célja az adatvédelmi és a magánéletet érintő kockázatok csökkentése, és amelyek segíthetnek megakadályozni az európai polgárok magánéletére és az adatvédelemhez fűződő alapvető jogukra gyakorolt kedvezőtlen hatások kialakulását.

AZ EGYÉNEKNEK A SZEMÉLYES ADATOK FELDOLGOZÁSA TEKINTETÉBEN VALÓ VÉDELMÉVEL FOGLALKOZÓ MUNKACSOPORT,

amelyet az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelv hozott létre,

tekintettel a fenti irányelv 29. cikkére, valamint 30. cikke (1) bekezdésének a) pontjára és (3) bekezdésére,

tekintettel a munkacsoport eljárási szabályzatára,

ELFOGADTA EZT A VÉLEMÉNYT:

1. A vélemény hatálya

A biometriáról szóló 2003. évi munkadokumentumban (WP80) a 29. cikk szerinti adatvédelmi munkacsoport (a továbbiakban: munkacsoport) feltárta a biometrikus adatok elektronikus olvasására és feldolgozására képes jövőbeli technológiák használatához kapcsolódó adatvédelmi kérdéseket. Az azóta eltelt évek során az ilyen technológia alkalmazása széles körűvé vált mind a köz-, mind a magánszférában, és több új szolgáltatás fejlődött ki. A korábban jelentős pénzügyi vagy számítástechnikai forrásokat igénylő biometrikus technológiák lényegesen olcsóbbá és gyorsabbá váltak. Az ujjlenyomat-olvasók használata ma már mindennapos. Egyes laptopok például beépített ujjlenyomat-olvasóval rendelkeznek a biometrikus hozzáférés-ellenőrzéshez. A DNS-elemzés terén történt előrelépéseknek köszönhetően az eredmények ma már pár percen belül rendelkezésre állnak. Egyes újonnan kifejlesztett technológiák – mint amilyen az érmintázat-felismerés vagy az arcfelismerés – máris kiforrottak. Hamarosan alkalmazni fogják őket mindennapi életünk különböző területein. A biometrikus technológiák szorosan kapcsolódnak egy egyén bizonyos jellemzőihez, és egyes technológiák felhasználhatók különleges adatok felfedésére. Emellett sok biometrikus technológia lehetővé teszi a személyek automatikus nyomon követését, felkutatását vagy a profilalkotást, ezért az egyének magánéletére és adatvédelemhez való jogára gyakorolt potenciális hatásuk jelentős. Ez a hatás az ilyen technológiák egyre terjedő alkalmazásával növekszik. Valószínű, hogy minden egyén bekerül egy vagy több biometrikus rendszerbe.

E vélemény célja, hogy felülvizsgált és naprakész keretet nyújtson a magánélet-védelmi és adatvédelmi elvek biometrikus alkalmazásokban való megvalósítására vonatkozó egységesített általános iránymutatásokkal és ajánlásokkal kapcsolatban. E vélemény címzettjei az európai és nemzeti jogalkotó hatóságok, a biometrikus rendszerek ágazata és az ilyen technológiák felhasználói.

2. Fogalommeghatározások

A biometrikus technológiák nem új keletűek, a munkacsoport különböző véleményei már tárgyalták őket. E rész célja, hogy összegyűjtse a vonatkozó meghatározásokat, és szükség esetén naprakésszé tegye azokat.

Biometrikus adat: ahogyan a munkacsoport a 4/2007. sz. véleményben (WP136) már kifejtette, a biometrikus adatok a következőképpen határozhatók meg:

„biológiai jellegzetességekként, viselkedési vonatkozásokként, pszichológiai sajátosságokként, életvitelként vagy olyan ismétlődő tevékenységekként, amelyek során e jellegzetességek és/vagy tevékenységek egyaránt egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is."

A biometrikus adatok visszavonhatatlanul megváltoztatják a test és a személyazonosság közötti kapcsolatot, mivel az emberi test jellemzőit gép által leolvashatóvá és további felhasználásra alkalmassá teszik.

A biometrikus adatok különböző formákban tárolhatók és dolgozhatók fel. Az egy személyre vonatkozóan rögzített biometrikus információkat néha olyan nyers adatok formában tárolják és dolgozzák fel, amelyek lehetővé teszik, hogy speciális ismeretek nélkül is felismerjék az információk forrását, ilyenek például az arcról készült fényképek, az ujjlenyomat-fényképek vagy a hangfelvételek. Más esetekben a rögzített nyers biometrikus információkat úgy dolgozzák fel, hogy csak bizonyos jellemzőket, illetve vonásokat nyernek ki és mentenek el biometrikus sablonként.

A biometrikus adatok forrása: a biometrikus adatok forrásai nagy változatosságot mutathatnak, és közéjük tartoznak az egyének fizikai, fiziológiai, viselkedési vagy pszichológiai összetevői. A 4/2007. sz. vélemény (WP136) szerint:

„a biometrikus adatok forrásai (például az emberi szövetminták) önmagukban nem tekinthetők biometrikus adatnak, de felhasználhatók biometrikus adatok gyűjtésére (az információ belőlük való kinyerése útján)."

A WP80. sz. dokumentumban megállapítottak szerint a biometrikus technikáknak két fő kategóriájuk van.

- Egyrészről vannak **fizikai** és fiziológiai alapú technikák, amelyek a személyek fizikai és fiziológiai jellemzőit vizsgálják, ezek közé tartozik az ujjlenyomat-ellenőrzés, az ujjkép-elemzés, az íriszfelismerés, a retinaelemzés, az arcfelismerés, a kézkörvonal-minták, a fülforma-felismerés, a testszagészlelés, a hangfelismerés, a DNS-mintázat elemzése és a verejtékpórus-elemzés stb.
- Másrészről vannak **viselkedésen** alapuló technikák, amelyek a személyek viselkedését mérik, ezek közé tartozik a kézzel írt aláírás ellenőrzése, a gépírás elemzése, a járás elemzése, a járásmód vagy a mozgás módja, a valamilyen tudatalatti gondolatra, például hazugságra utaló mintázatok stb.

Figyelembe kell venni a **pszichológiai** alapú technikák egyre fejlődő területét is. Ide tartozik a konkrét helyzetekre adott válasz mérése vagy a valamilyen pszichológiai profilnak való megfelelést mérő speciális tesztek.

Biometrikus sablon: a nyers biometrikus adatokból kulcsfontosságú jellemzőket lehet kinyerni (például az arc mért adatait egy képből), és a nyers adat helyett ezeket lehet eltárolni későbbi feldolgozásra. Ez képezi az adatok biometrikus sablonját. A sablon méretének (az információk mennyiségének) a meghatározása döntő fontosságú kérdés. A sablon méretének egyrészről elég nagynak kell lennie a biztonságos működéshez (a különböző biometrikus adatok közötti átfedésnek vagy a személyazonosságok felcserélésének az elkerülése), másrészről a sablon mérete nem lehet túl nagy, elkerülendő a biometrikus adatok

rekonstrukciójának kockázatát. A sablon generálásának egyirányú folyamatnak kell lennie, a nyers biometrikus adatok visszanyerését nem szabad lehetővé tenni a sablonból.

Biometrikus rendszerek: a WP80. sz. dokumentum szerint a biometrikus rendszerek:

> *„olyan biometrikus technológiákat használó alkalmazások, amelyek lehetővé teszik a személyek automatikus azonosítását, illetve hitelesítését/ellenőrzését. A hitelesítési/ellenőrzési alkalmazásokat gyakran használják különféle feladatokra nagyon eltérő területeken, különböző célokból, és nagyon sokféle különböző jogalany felelősségi körében."*

A közelmúltbeli technológiai fejleményeknek köszönhetően ma már kategorizálási/elkülönítési célokra is lehet használni a biometrikus rendszereket.

A biometrikus rendszerek jelentette kockázatok a feldolgozás során használt biometrikus adatok jellegéből fakadnak. Ezért általánosabb meghatározás lenne, ha olyan rendszerről beszélnénk, amely biometrikus adatok kinyerését és további feldolgozását végzi.

A biometrikus adatok biometrikus rendszerben történő feldolgozása tipikusan különböző folyamatokat foglal magában, mint amilyen a felvétel, a tárolás és a megfeleltetés:

– **Biometrikus felvétel:** magában foglalja mindazokat a folyamatokat, amelyeket egy biometrikus rendszeren belül a biometrikus adatok valamely biometrikus forrásból való kinyerése és azoknak egy egyénhez való kapcsolása érdekében végeznek. A felvétel során szükséges adatok mennyiségének és minőségének megfelelőnek kell lennie ahhoz, hogy lehetővé tegye az egyén pontos azonosítását, hitelesítését, kategorizálását vagy ellenőrzését anélkül, hogy túl sok adatot rögzítenének. A felvételi szakasz során a biometrikus forrásból kinyert adatok mennyiségének meg kell felelnie a feldolgozás céljának és a biometrikus rendszer teljesítményszintjének.

A felvételi szakasz tipikusan az első alkalom, amikor egy egyén kapcsolatba kerül egy adott biometrikus rendszerrel. A felvételhez a legtöbb esetben az egyén személyes közreműködése szükséges (például ujjlenyomatvétel esetén), ami megfelelő alkalmat adhat a tájékoztatásra és a tisztességes adatfeldolgozásról szóló értesítésre. Lehetséges azonban az egyének felvétele a tudomásuk vagy a hozzájárulásuk nélkül is (például beágyazott arcfelismerő funkcióval rendelkező CCTV-rendszerek). A felvételi folyamat pontossága és biztonsága alapvető fontosságú az egész rendszer teljesítménye szempontjából. Előfordulhat az egyén biometrikus rendszerbe való felvételének megismétlése a nyilvántartott biometrikus adatok naprakésszé tétele érdekében.

– **Biometrikus tárolás:** a felvétel során megszerzett adatok későbbi felhasználás céljából tárolhatók helyben, abban a műveleti központban, ahol a felvételre sor került (például egy olvasóban), vagy az egyén által hordozott valamely eszközön (például egy intelligens kártyán), illetve elküldhető tárolásra egy központosított adatbázisba, amely hozzáférhető egy vagy több biometrikus rendszer számára.

– **Biometrikus megfeleltetés:** ez az a folyamat, amelynek során a (felvételkor rögzített) biometrikus adatokat/sablont összevetik egy új mintából gyűjtött biometrikus adatokkal/sablonnal azonosítás, ellenőrzés/hitelesítés vagy kategorizálás céljából.

Biometrikus azonosítás: az egyén biometrikus rendszer általi azonosítása tipikusan az egyén (azonosításkor megszerzett) biometrikus adatainak adatbázisban tárolt több biometrikus sablonnal való összehasonlításának folyamata (azaz egy a többhöz megfeleltetési folyamat).

Biometrikus ellenőrzés/hitelesítés: az egyén biometrikus rendszer általi ellenőrzése tipikusan az egyén (ellenőrzéskor megszerzett) biometrikus adatainak egy eszközön tárolt valamely biometrikus sablonnal való összehasonlításának folyamata (azaz egy az egyhez megfeleltetési folyamat).

Biometrikus kategorizálás/elkülönítés: az egyén biometrikus rendszer általi kategorizálása/elkülönítése tipikusan az a folyamat, amelynek során egy konkrét cselekmény elvégzése érdekében megállapítják, hogy az egyén biometrikus adatai beletartoznak-e egy előre meghatározott jellemzőkkel bíró csoportba. Ebben az esetben nem az egyén azonosítása vagy ellenőrzése a fontos, hanem az, hogy automatikusan egy bizonyos kategóriába sorolják be. Egy reklámfelület például kor vagy nem alapján különböző reklámokat mutathat attól függően, hogy ki nézi a reklámokat.

Multimodális biometrikus technológiák: ezek a különböző biometrikus technológiák kombinációiként határozhatók meg a rendszer pontosságának vagy teljesítményének javítása érdekében (többszintű biometrikus technológiáknak is nevezik őket). A biometrikus rendszerek ugyanazon egyéntől származó két vagy több biometrikus vonást/jellemzőt használnak a megfeleltetési folyamatban. Ezek a rendszerek különféleképpen működhetnek, vagy különböző biometrikus adatokat gyűjtenek különböző érzékelőkkel, vagy ugyanazon biometrikus adatból gyűjtenek több egységet. Egyes tanulmányok ebbe a kategóriába sorolják azokat a rendszereket is, amelyek ugyanazon biometrikus adatok többszörös leolvasásával működnek, vagy több algoritmust használnak ugyanazon a biometrikus mintán a jellemzők kinyerésére. A multimodális biometrikus rendszerekre példa az ePassport uniós szinten, valamint az US-VISIT biometrikus azonosítási szolgáltatások az Egyesült Államokban.

Pontosság: biometrikus rendszerek használatakor nehéz 100 %-ban hibamentes eredményeket produkálni. Ez lehet az adat megszerzésekor jellemző környezeti viszonyok eltérései miatt (világítás, hőmérséklet stb.) és a használt berendezések (kamerák, szkennelő eszközök stb.) különbségei miatt is. A leggyakrabban használt, szokásos teljesítményértékelési mérőszámok a hibás elfogadási arány és a hibás elutasítási arány, amelyek hozzáigazíthatók a használt rendszerhez:

– A hibás elfogadási arány (False Accept Rate, FAR): annak a valószínűsége, hogy a biometrikus rendszer tévesen azonosít valakit, vagy nem utasít el egy csalót. A hibásan elfogadott érvénytelen bevitelek százalékos arányát méri. Nevezik hamis pozitív aránynak is.

– A hibás elutasítási arány (False Reject Rate, FRR): annak a valószínűsége, hogy a rendszer hibás elutasítást végez. Hibás elutasítás akkor történik, ha egy egyént nem rendelnek hozzá a saját meglévő biometrikus sablonjához. Nevezik hamis negatív aránynak is.

Megfelelő rendszerhangolás és beállítások mellett a biometrikus rendszerek kritikus hibáit az operatív működésre vonatkozóan engedélyezett szintre lehet minimalizálni a helytelen értékelések kockázatának csökkentése révén. Egy tökéletes rendszerben nulla a hibás elfogadási és a hibás elutasítási arány, de gyakoribb, hogy negatív összefüggés áll fenn

köztük. A hibás elfogadási arány növekedése gyakran csökkenti a hibás elutasítási arány szintjét.

Annak vizsgálatakor, hogy a biometrikus rendszer pontossága elfogadható-e vagy sem, fontos értékelni a feldolgozás célját, a hibás elutasítási és hibás elfogadási arányt, valamint a populáció méretét. Ezenkívül a biometrikus rendszer pontosságának vizsgálata során figyelembe lehet venni az élő minta észlelésére vonatkozó képességet. Például a látens ujjlenyomatok lemásolhatók és felhasználhatók hamis ujjak létrehozásához. Egy ujjlenyomat-olvasó ilyen esetben nem tévedhet, és nem végezhet pozitív azonosítást.

3. Jogi elemzés

A vonatkozó jogi keret az adatvédelmi irányelv (95/46/EK). A munkacsoport a WP80. sz. dokumentumban már megállapította, hogy a biometrikus adatok a legtöbb esetben személyes adatok. Ezért csak akkor dolgozhatók fel, ha van rá jogalap, és ha a gyűjtésük, illetve további feldolgozásuk célja szempontjából a feldolgozás megfelelő, releváns és nem túlzott mértékű.

Cél

A biometria használatának előfeltétele a biometrikus adatok gyűjtése és feldolgozása céljának egyértelmű meghatározása, figyelembe véve az egyének alapvető jogainak és szabadságának védelmét érintő kockázatokat.

Gyűjthetők például biometrikus adatok annak érdekében, hogy a személyes adatok engedély nélküli hozzáférés elleni védelmét szolgáló megfelelő intézkedések végrehajtásával biztosítsák vagy növeljék a feldolgozórendszerek biztonságát. Elvileg nincs akadálya annak, hogy a feldolgozást irányító személyek biometrikus jellemzőin alapuló megfelelő biztonsági intézkedéseket vezessenek be annak érdekében, hogy biztosított legyen a feldolgozás jelentette kockázatoknak és a védendő személyes adatok természetének megfelelő szintű biztonság. Nem szabad azonban megfeledkezni arról, hogy a biometria alkalmazása önmagában nem biztosít nagyobb biztonságot, mivel sok biometrikus adat gyűjthető az érintett személy tudtán kívül. Minél magasabb a tervezett biztonsági szint, annál kevésbé képesek önmagukban a biometrikus adatok elérni a kitűzött célt.

Be kell tartani a célhoz kötöttség elvét és a többi adatvédelmi elvet; különösen az arányosság, a szükségesség és az adatminimalizálás elvét kell észben tartani, amikor egy alkalmazás különféle céljainak meghatározására kerül sor. Ha lehetséges, az érintettnek mindig választási lehetőséget kell biztosítani a több funkcióval rendelkező alkalmazás számos célja között, különösen, ha e célok közül egyhez vagy többhöz biometrikus adatok feldolgozása szükséges.

Példa:
Biometrikus adatokon alapuló sajátos hitelesítési eljárásokat nyújtó elektronikus eszközök alkalmazását javasolták azokkal a biztonsági intézkedésekkel kapcsolatban, amelyeket a következő esetekben kell meghozni:
- a telefonszolgáltatók által bírósági engedéllyel végzett lehallgatási tevékenység során gyűjtött személyes adatok feldolgozása;
- mind a nyilvánosan elérhető elektronikus hírközlési szolgáltatók vagy nyilvános hírközlési hálózatok üzemeltetői által igazságszolgáltatási célból megőrzött forgalmi (és helyre vonatkozó) adatokhoz való hozzáférés, mind az ilyen adatok tárolására szolgáló helyiségekhez való hozzáférés;

- genetikai adatok és biológiai minták gyűjtése és tárolása.

Az interneten, a közösségi médiában, az online fényképkezelő vagy megosztó alkalmazásokban található **fényképek** nem dolgozhatók fel tovább biometrikus sablonok kinyerése vagy biometrikus rendszerbe való, a képeken szereplő személyek automatikus felismerését (arcfelismerés) szolgáló felvétel érdekében anélkül, hogy ennek az új célnak konkrét jogalapja lenne (például hozzájárulás). Ha van jogalapja az ilyen másodlagos célnak, akkor a feldolgozásnak emellett e cél szempontjából megfelelőnek, relevánsnak és nem túlzott mértékűnek kell lennie. Ha az érintett hozzájárul ahhoz, hogy a fényképek, amelyeken megjelenik, arcfelismerő algoritmust használó online fényképalbumban az ő automatikus megjelölésével feldolgozhatók legyenek, akkor ezt az adatvédelmi szabályozást szem előtt tartva kell végrehajtani: a képeknek a névvel, becenévvel vagy az érintett által meghatározott bármilyen más szöveggel való megjelölése után már nem szükséges adatokat törölni kell. Ehhez a célhoz nem szükséges állandó biometrikus adatbázis előzetes létrehozása.

Arányosság

A biometria használata felveti annak a problémáját, hogy az adatfeldolgozás célja alapján a feldolgozott adatok minden kategóriája arányos-e. Mivel a biometrikus adatokat csak akkor lehet használni, ha megfelelőek, relevánsak és nem túlzott mértékűek, ezzel együtt jár annak szigorú értékelése, hogy a feldolgozott adatok szükségesek és arányosak-e, és hogy a kitűzött cél elérhető lenne-e kisebb beavatkozással járó módon is.

Egy javasolt 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.[1] 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 érhető 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[2].

Példa:
Egy egészség- és fitneszklubban az ujjlenyomatok gyűjtésén alapuló központosított biometrikus rendszert vezetnek be, hogy az edzőterem helyiségeihez és a kapcsolódó szolgáltatásokhoz csak azok a vendégek kapjanak hozzáférést, akik megfizették a díjat.
Egy ilyen rendszer működtetéséhez szükséges lenne, hogy tárolják az összes vendég és a személyzet valamennyi tagjának az ujjlenyomatát. Ez a biometrikus alkalmazás aránytalannak

[1] A biometriát ellenőrzési vagy azonosítási célból fogják használni: egy biometrikus azonosító technikailag megfelelőnek bizonyulhat az egyik célra, és nem megfelelőnek a másikra (például azokat a technológiákat, amelyekre alacsony hibás elutasítási arány jellemző, előnyben kell részesíteni azon rendszerek esetében, amelyeket a bűnüldözés terén való azonosítás céljára alakítottak ki).

[2] Például intelligens kártyák vagy más olyan módszerek, amelyek nem gyűjtenek vagy központosítanak biometrikus információkat hitelesítési célból.

tűnik ahhoz az igényhez képest, hogy ellenőrizzék a klubba való belépést és megkönnyítsék a bérletek kezelését. Könnyen elképzelhető, hogy ugyanannyira megvalósíthatók és hatékonyak lennének olyan, biometrikus adatok feldolgozását nem igénylő egyéb intézkedések is, mint egy egyszerű lista, illetve az RFID-címkék vagy a lehúzós kártyák használata.

A munkacsoport figyelmeztet azokra a kockázatokra, amelyek a biometrikus adatok azonosítási célú használatával járnak nagy, központosított adatbázisok használata esetén, tekintettel az érintett személyekre vonatkozó, potenciálisan káros következményekre.

Figyelembe kell venni, hogy az ilyen rendszerek jelentős befolyással vannak az érintettek emberi méltóságára, és tekintetbe kell venni e rendszerek alapvető jogokhoz kapcsolódó vonatkozásait. Az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény és az Emberi Jogok Európai Bíróságának az egyezmény 8. cikkével kapcsolatos ítélkezési gyakorlata alapján a munkacsoport hangsúlyozza, hogy az adatvédelemhez való jogba történő bármilyen beavatkozás csak azzal a feltétellel engedélyezhető, ha az megfelel a jognak, és a demokratikus társadalomban fontos közérdek megvédéséhez szükséges[3].

E feltételek betartásának biztosításához meg kell határozni azt a célt, amelyet a rendszer szolgál, és meg kell vizsgálni, hogy a rendszerben rögzítendő adatok arányosak-e az említett célhoz képest.

Ennek érdekében az adatkezelőnek meg kell állapítania, hogy a feldolgozás és annak mechanizmusai, a gyűjtendő és feldolgozandó adatok kategóriái, valamint az adatbázisban található információk továbbítása szükséges és elengedhetetlen-e. Az elfogadott biztonsági intézkedéseknek megfelelőnek és hatékonynak kell lenniük. Az adatkezelőnek figyelembe kell vennie az azoknak az egyéneknek biztosítandó jogokat, akikre a személyes adatok vonatkoznak, és biztosítania kell, hogy az alkalmazásnak részét képezze az ilyen jogok gyakorlására alkalmas megfelelő mechanizmus.

Példa:
A biometrikus adatok azonosítási célú felhasználása. A személyek arcát vagy DNS-ét elemző rendszerek nagyon hatékonyan járulhatnak hozzá a bűncselekmények elleni küzdelemhez, és hatékonyan fedhetik fel egy súlyos bűncselekménnyel gyanúsított ismeretlen személy személyazonosságát. E rendszerek kiterjedt alkalmazása azonban súlyos veszélyeket is hordoz magában. Az arcfelismerés esetében, amelynek során a biometrikus adatok könnyen rögzíthetők az érintett tudomása nélkül is, a széles körű használat megszüntetné az anonimitást a közterületeken, és lehetővé tenné az egyének következetes nyomon követését. A DNS-adatok esetében a technológia használata azzal a veszéllyel jár, hogy az egyén egészségére vonatkozóan különleges adatok derülhetnek ki.

[3] Lásd az Európai Unió Bíróságának a C-465/00., C-138/01. és C-139/01. sz. (Rechnungshof kontra Österreichischer Rundfunk és mások) egyesített ügyekben 2003. május 20-án hozott ítéletét, az Emberi Jogok Európai Bíróságának a 30562/04. és 30566/04. sz. (S. és Marper kontra Egyesült Királyság) ügyben 2008. december 4-én hozott ítéletét és a 30089/04., 14449/06., 24968/07., 13870/08., 36363/08., 23499/09., 43852/09. és 64027/09. sz. ügyben (Goggins és mások kontra Egyesült Királyság) 2011. július 19-én hozott ítéletét.

Pontosság

A feldolgozott biometrikus adatoknak a gyűjtésük céljával arányosan pontosnak és relevánsnak kell lenniük. Az adatoknak pontosnak kell lenniük a felvételkor, illetve a személy és a biometrikus adatok közötti kapcsolat létrehozásakor is. A felvételkor a pontosság jelentőséggel bír a személyazonossággal való csalás megelőzése szempontjából is.

A biometrikus adatok egyediek, és legtöbbjük egyedi sablont vagy képet generál. Ha széles körben használják őket, különösen, ha a populáció jelentős részére vonatkozóan, akkor a biometrikus adatok a 95/46/EK irányelv értelmében vett általános jellegű azonosító jeleknek tekinthetők. Ilyen esetben alkalmazandó lenne a 95/46/EK irányelv 8. cikkének (7) bekezdése, és a tagállamoknak kellene meghatározniuk a jelek feldolgozásának feltételeit.

Adatminimalizálás

Sajátos problémát vethet fel, hogy a biometrikus adatok gyakran több információt tartalmaznak annál, mint ami a megfeleltető függvényekhez szükséges. Az adatminimalizálás elvét az adatkezelőnek kell végrehajtatnia. Ez egyrészről azt jelenti, hogy az összes rendelkezésre álló információ helyett csak a szükséges információkat szabad feldolgozni, továbbítani vagy tárolni. Másrészről pedig az adatkezelőnek gondoskodnia kell arról, hogy az alapbeállítás kényszerítő körülmények nélkül mozdítsa elő az adatvédelmet.

Megőrzési időszak

Az adatkezelőnek megőrzési időszakot kell meghatároznia a biometrikus adatokra vonatkozóan, amely nem lehet hosszabb, mint az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges idő. Az adatkezelőnek biztosítania kell, hogy az adatokat vagy az ilyen adatokból származtatott profilokat véglegesen töröljék ennek az indokolt időszaknak az eltelte után.

Egyértelműnek kell lennie a különbségnek az általános személyes adatok között, amelyekre lehet, hogy hosszabb ideig van szükség, és a biometrikus adatok között, amelyeknek már nincs hasznuk, például ha az érintettnek már nem biztosítanak hozzáférést egy bizonyos területhez.

Példa:
Egy munkáltató biometrikus rendszert működtet egy korlátozott területre való belépés ellenőrzésére. Egyik munkavállalójának szerepe a továbbiakban már nem teszi szükségessé, hogy belépjen a korlátozott területre (például megváltozik a felelősségi köre vagy a munkaköre). Ebben az esetben a munkavállaló biometrikus adatait törölni kell, mivel megszűnt az adatgyűjtés célja.

3.1. Jogszerű indok

A biometrikus adatok feldolgozásának a 95/46/EK irányelv 7. cikkében foglalt jogszerű indokok egyikén kell alapulnia.

3.1.1. Hozzájárulás, 7. cikk, a) pont

A jogszerűség első ilyen, a 7. cikk a) pontjában szereplő indoka az, ha az érintett hozzájárulását adta az adatfeldolgozáshoz. Az adatvédelmi irányelv 2. cikkének h) pontja szerint a hozzájárulás az érintett kívánságának önkéntes, kifejezett és tájékozott kinyilvánítása kell, hogy legyen. Egyértelműnek kell lennie, hogy ilyen hozzájárulás nem szerezhető meg önkéntesen az általános szerződési feltételek kötelező elfogadása vagy kívülmaradási

lehetőségek útján. A hozzájárulásnak ezenkívül visszavonhatónak kell lennie. Ezzel kapcsolatban a munkacsoport a hozzájárulás meghatározásáról szóló véleményében hangsúlyozza a fogalom különböző fontos vonatkozásait: a hozzájárulás érvényességét; az egyéneknek a hozzájárulás visszavonásához való jogát; a feldolgozás megkezdése előtt adott hozzájárulást; a tájékoztatás minőségére és hozzáférhetőségére vonatkozó követelményeket[4].

Sok olyan esetben, amikor biometrikus adatokat dolgoznak fel, érvényes alternatíva – például útlevél vagy lehúzós kártya – hiányában a hozzájárulást nem lehetne önkéntesen megadottnak tekinteni. Egy olyan rendszert például, amely elrettenti az érintetteket a használatától (például a felhasználó túl sok idejét veszi igénybe vagy túl bonyolult), nem lehetne érvényes alternatívának tekinteni, és így nem eredményezne érvényes hozzájárulást.

Példák:
Egyéb alternatív jogszerű indokok hiányában videoklubba való belépés ellenőrzésére csak abban az esetben használható biometrikus hitelesítési rendszer, ha a fogyasztók szabadon dönthetnek arról, hogy igénybe veszik-e ezt a rendszert. Ez azt jelenti, hogy a filmklub tulajdonosának alternatív, a magánéletbe kevésbé beavatkozó mechanizmusokat kell elérhetővé tennie. Egy ilyen rendszer lehetővé teszi, hogy azok a fogyasztók, akik személyes körülményeik miatt nem akarnak vagy nem képesek ujjlenyomatot adni, megtagadhassák hozzájárulásukat. Ha csak a szolgáltatás igénybevételéről való lemondás és a biometrikus adatok szolgáltatása között lehet választani, az jelentős mértékben utal arra, hogy a hozzájárulás megadása nem önkéntesen történt, és nem tekinthető jogszerű indoknak.

Egy óvodában érmintázat-szkennert helyeznek üzembe, hogy minden belépő felnőtt (a szülők és a személyzet tagjai) esetében ellenőrizzék a belépésre való jogosultságot. Egy ilyen rendszer működtetéséhez szükséges lenne, hogy tárolják az összes szülő és a személyzet valamennyi tagjának az ujjlenyomatát. A hozzájárulás megkérdőjelezhető jogalapot képezne, különösen a munkavállalók esetében, mivel előfordulhat, hogy nem rendelkeznek valódi választási lehetőséggel egy ilyen rendszer használatának elutasítására vonatkozóan. A szülők esetében is megkérdőjelezhető lenne, amennyiben nincs alternatív módja az óvodába való belépésnek.

Bár kifejezetten vélelmezhető, hogy a munkáltató és a munkavállaló között általában fennálló egyenlőtlen helyzet miatt a hozzájárulás határozottsága megkérdőjelezhető, a munkacsoport nem zárja ki teljesen: *„amennyiben kellően garantált, hogy a hozzájárulás valóban önkéntes”*[5].

A foglalkoztatás terén tehát meg kell kérdőjelezni a hozzájárulást, és annak megfelelően indokoltnak kell lennie. Hozzájárulás kérése helyett a munkáltatók megvizsgálhatnák, hogy jogszerű cél érdekében, igazolhatóan szükséges-e a munkavállalók biometrikus adatainak használata, és mérlegelhetnék ennek a szükségszerűségét a munkavállalók alapvető jogai és szabadsága szempontjából. Azokban az esetekben, amelyekben a szükségszerűség megfelelően indokolható, az ilyen feldolgozás jogalapja alapulhat az adatkezelő jogszerű érdekén, ahogyan azt a 95/46/EK irányelv 7. cikkének f) pontja meghatározza.
A munkáltatónak mindig a legkisebb beavatkozással járó módszerre kell törekednie azáltal, hogy lehetőség szerint nem biometrikus eljárást választ.

4 WP 187, 15/2011. sz. vélemény a hozzájárulás meghatározásáról.

5 WP 187, 15/2011. sz. vélemény a hozzájárulás meghatározásáról.

A 3.1.3. pontban leírtak szerint azonban lehetnek olyan esetek, amelyekben a biometrikus rendszer az adatkezelő jogszerű érdekét szolgálhatja. Ezekben az esetekben nem lenne szükséges a hozzájárulás.

A hozzájárulás csak akkor érvényes, ha kellő tájékoztatást adnak a biometrikus adatok felhasználásáról. Mivel a biometrikus adatok használhatók egyedi és univerzális azonosítóként, a konkrét adatok felhasználására vonatkozó egyértelmű és könnyen hozzáférhető tájékoztatást abszolút szükségesnek kell tekinteni a tisztességes feldolgozás biztosításához. Ezért ez az érvényes hozzájárulás elengedhetetlen feltétele a biometrikus adatok felhasználásának.

Példák:
Egy ujjlenyomatokat használó hozzáférés-ellenőrzési rendszerhez való érvényes hozzájáruláshoz tájékoztatás szükséges arra vonatkozóan, hogy a biometrikus rendszer olyan sablont hoz-e létre, amely csak az adott rendszerre jellemző. Ha olyan algoritmust használnak, amely ugyanazt a biometrikus sablont hozza létre különböző biometrikus rendszerekben, az érintettnek tudnia kell, hogy számos különböző biometrikus rendszerben felismerhetik.

Valaki feltölti a fényképét egy internetes fényképalbumba. Ahhoz, hogy ez a kép bekerüljön egy biometrikus rendszerbe, kifejezett hozzájárulás szükséges, amely az arra vonatkozó kimerítő tájékoztatáson alapul, hogy mi történik a biometrikus adatokkal és mennyi ideig, milyen célokból dolgozzák fel őket.

Mivel a hozzájárulás bármikor visszavonható, az adatkezelőknek olyan technikai megoldásokat kell megvalósítaniuk, amelyek visszafordíthatják a biometrikus adatok rendszereikben való használatát. A hozzájárulás alapján működő biometrikus rendszereknek tehát képesnek kell lenniük arra, hogy hatékonyan megszüntessenek minden általuk létrehozott személyazonossági kapcsolatot.

3.1.2. Szerződés, 7. cikk, b) pont

A biometrikus adatok feldolgozása szükséges lehet olyan szerződés teljesítéséhez, amelyben az érintett az egyik fél, vagy szükséges lehet a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez. Meg kell azonban jegyezni, hogy ez általában csak arra az esetre vonatkozik, ha pusztán biometrikus szolgáltatásokat nyújtanak. Ez a jogalap nem használható fel arra, hogy olyan másodlagos szolgáltatást tegyen jogszerűvé, amely az adott személy valamely biometrikus rendszerbe való felvételéből áll. Ha az ilyen szolgáltatás elválasztható a főszolgáltatástól, akkor a főszolgáltatásra vonatkozó szerződés nem teheti jogszerűvé a biometrikus adatok feldolgozását. A személyes adatok nem termékek, amelyeket szolgáltatásért cserébe lehet kérni, így azok a szerződések, amelyek ezeket tartalmazzák, illetve azok a szerződések, amelyek csak azzal a feltétellel kínálnak szolgáltatást, hogy valaki hozzájárul a biometrikus adatainak egy másik szolgáltatás céljából való feldolgozásához, nem szolgálhatnak jogalapul ehhez a feldolgozáshoz.

Példák:
a) Két testvér hajmintákat ad egy laboratóriumnak DNS-teszt céljából, hogy kiderüljön, valóban testvérek-e. A laboratóriummal kötött, az adott teszt elvégzésére vonatkozó szerződés kellő jogalapot jelent a felvételhez és a biometrikus adatok feldolgozásához.

b) Valaki feltölt egy fényképet egy közösségi hálózaton lévő fényképalbumába, hogy megmutassa a barátainak. Ha a szerződés (szolgáltatási feltételek) azt írja elő, hogy a szolgáltatás igénybevétele az adott felhasználó biometrikus rendszerbe történő felvételéhez kötött, akkor ez az előírás nem elegendő jogalap ehhez a felvételhez.

3.1.3. Jogi kötelezettség, 7. cikk, c) pont

A személyes adatok feldolgozásának egy másik jogalapja, ha a feldolgozás az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Ez a helyzet például egyes országokban útlevelek[6] és vízumok[7] kibocsátása, illetve használata esetén.

3.1.4. Az adatkezelő jogszerű érdeke, 7. cikk, f) pont

A 95/46/EK irányelv 7. cikke szerint indokolt lehet a biometrikus személyes adatok feldolgozása akkor is, ha „az adatkezelő, vagy az adatokat megkapó harmadik fél, vagy felek jogszerű érdekének érvényesítéséhez szükséges, kivéve, ha ezeknél az érdekeknél magasabb rendűek az érintettnek az [...] érdekei az alapvető jogok és szabadságok tekintetében".

Ez azt jelenti, hogy vannak esetek, amikor a biometrikus rendszerek használata az adatkezelő jogszerű érdekét szolgálja. Az ilyen érdek azonban csak akkor jogszerű, ha az adatkezelő bizonyítani tudja, hogy az érdeke objektív módon magasabb rendű az érintett azon jogánál, hogy ne vegyék fel egy biometrikus rendszerbe. Ha például a magas kockázatú területek biztonságát kifejezetten olyan mechanizmussal kell biztosítani, amely képes pontosan ellenőrizni, hogy a személyek jogosultak-e belépni ezekre a területekre, akkor egy biometrikus rendszer használata az adatkezelő jogszerű érdekét szolgálhatja. Az alábbi példában, amely egy laboratórium biometrikus hozzáférés-ellenőrzési rendszeréhez kapcsolódik, az adatkezelő nem tud alternatív mechanizmust felkínálni a munkavállalónak anélkül, hogy az közvetlenül hatással lenne a korlátozás alatt álló terület biztonságára, mivel nincsenek alternatív, kisebb beavatkozással járó intézkedések, amelyek megfelelőek lennének az adott terület megfelelő biztonsági szintjének eléréséhez. Tehát az adatkezelő jogszerű érdekét szolgálja, hogy bevezesse a rendszert, és felvezessen abba néhány munkatársat. Ehhez nem kell megszereznie a hozzájárulásukat. Azonban abban az esetben, ha az adatkezelő jogszerű érdeke érvényes jogalap a feldolgozáshoz, az egyéb adatvédelmi elveket – mint mindig – továbbra is alkalmazni kell, különösen az arányosság és az adatminimalizálás elvét.

Példa:
Egy veszélyes vírusokat kutató vállalat egyik laboratóriumát olyan ajtók biztosítják, amelyek csak ujjlenyomat- és íriszszkennelés alapján történő sikeres ellenőrzést követően nyílnak ki. Azért vezették be ezt a rendszert, hogy biztosan csak a sajátos kockázatokat ismerő, az eljárások terén képzett és a vállalat által megbízhatónak talált személyek kísérletezhessenek ezekkel a veszélyes anyagokkal. A vállalat azon jogszerű érdeke, hogy az adott területhez való

---

6 Az ujjlenyomatokat a 2004. december 13-i 2252/2004/EK tanácsi rendeletnek megfelelően beillesztették az útlevelekbe, illetve a 2002. június 13-i 1030/2002/EK tanácsi rendeletnek megfelelően a tartózkodási engedélyekbe.

7 A biometrikus azonosítóknak a vízuminformációs rendszerben (VIS) történő rögzítését a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló, 2008. július 9-i 767/2008/EK rendelet (VIS-rendelet) alapozza meg. Lásd még a 3/2007. sz. véleményt a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2006) 269 végleges) WP 134; ezenkívül a 2/2005. sz. véleményt a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslatról (COM(2004) 835 végleges) WP 110; valamint a 7/2004. sz. véleményt a biometrikus elemek tartózkodási engedélyekben és vízumokban való szerepeltetéséről, figyelemmel az európai vízuminformációs rendszer (VIS) létrehozására; WP 96.

hozzáférésből eredő biztonsági kockázatok jelentős csökkenésének garantálása érdekében gondoskodjon arról, hogy csak bizonyos személyek léphessenek be egy korlátozás alatt álló területre, sokkal magasabb rendű az egyének azon kívánságánál, hogy ne dolgozzák fel a biometrikus adataikat.

A biometriának a tulajdon és az egyének általános biztonsági szükségletei kapcsán való használata főszabályként nem tekinthető az érintett érdekeinél vagy alapvető jogainál és szabadságánál magasabb rendű jogszerű érdeknek. Ellenkezőleg, a biometrikus adatok feldolgozása csak akkor indokolható azzal, hogy tulajdon, illetve egyének biztosításához szükséges eszköz, ha objektív és dokumentált körülmények alapján bizonyított, hogy ténylegesen jelentős kockázat áll fenn. Ehhez az adatkezelőnek bizonyítania kell, hogy egyes körülmények konkrét, jelentős kockázatot jelentenek, amelyet az adatkezelőnek különös gondossággal kell értékelnie. Annak érdekében, hogy megfeleljen az arányosság elvének, az adatkezelő ezekben a magas kockázattal járó helyzetekben köteles ellenőrizni, hogy egyes alternatív intézkedések lehetnének-e a kitűzött célra tekintettel ugyanolyan hatékonyak, de kisebb beavatkozással járók, és köteles ezeket az alternatívákat választani.
A szóban forgó körülményeket is rendszeresen felül kell vizsgálni. E felülvizsgálat eredménye alapján meg kell szüntetni vagy fel kell függeszteni minden olyan adatfeldolgozási műveletet, amelyről azt állapítják meg, hogy már nem indokolt.

3.2. Adatkezelő és adatfeldolgozó

A 95/46/EK irányelv kötelezettségeket állapít meg az adatkezelőkre vonatkozóan a személyes adatok általuk végzett feldolgozását illetően. A biometria terén különböző típusú jogi személyek lehetnek adatkezelők, például munkáltatók, bűnüldöző hatóságok vagy migrációs hatóságok.

A munkacsoport emlékeztet az adatkezelő és az adatfeldolgozó fogalmáról szóló véleményében[8] foglalt iránymutatásra, amely hatékonyan tisztázza, hogy hogyan kell értelmezni az irányelvnek ezeket az alapvető meghatározásait.

3.3. Automatizált feldolgozás (az irányelv 15. cikke)

Biometrikus adatok feldolgozásán alapuló rendszerek használatakor különös figyelmet kell fordítani a rendszer által elutasított személyeket érintő lehetséges, megkülönböztetéssel járó következményekre. Az egyének azon joga védelmének érdekében ezenkívül, hogy kizárólag automatikus adatfeldolgozás alapján ne vonatkozzon rájuk őket érintő intézkedés, megfelelő biztosítékokat kell bevezetni, például emberi beavatkozást, jogorvoslatokat vagy olyan mechanizmusokat, amelyek lehetővé teszik az érintettek számára, hogy ismertessék álláspontjukat.

A 95/46/EK irányelv 15. cikke szerint *„A tagállamok minden személynek biztosítják a jogot arra, hogy ne terjedhessen ki rájuk olyan döntés hatálya, amely rájuk nézve jogi hatással járna, vagy őket jelentős mértékben érintené, és amely kizárólag automatizált feldolgozáson alapul, és amelynek célja a rá vonatkozó egyes olyan személyes szempontok kiértékelése, mint például a munkahelyi teljesítmény, a hitelképesség, a megbízhatóság, az életvitel stb.”*

[8] WP169, 1/2010. sz. vélemény az „adatkezelő” és az „adatfeldolgozó” fogalmáról.

3.4. Áttekinthetőség és az érintett tájékoztatása

A tisztességes adatfeldolgozás elve értelmében az érintetteknek tudatában kell lenniük annak, hogy gyűjtik, illetve feldolgozzák a biometrikus adataikat (a 95/46/EK irányelv 6. cikke). Kerülendő minden olyan rendszer, amely az érintett tudtán kívül gyűjtene ilyen adatokat.

Az adatkezelőnek gondoskodnia kell arról, hogy az érintetteket az adatvédelmi irányelv 10. cikkével összhangban megfelelően tájékoztassák az adatfeldolgozás legfontosabb elemeiről, mint amilyen az adatkezelő személye, az adatfeldolgozás célja, az adatok típusa, a feldolgozás időtartama, az érintetteknek az adataikba való betekintéshez és az adatok helyesbítéséhez vagy törléséhez való joga, a hozzájárulás visszavonásának joga, valamint az adatok címzettjeire, illetve a címzettek kategóriáira vonatkozó tájékoztatás. Mivel a biometrikus rendszerek irányítóinak kötelességük tájékoztatni az érintetteket, a tudomásuk nélkül senkitől nem lehet biometrikus adatokat levenni.

3.5. A biometrikus adatokhoz való hozzáférés joga

Az érintetteknek joguk van ahhoz, hogy az adatkezelőktől hozzáférést kapjanak az adataikhoz, általában a biometrikus adataikhoz is. Az érintetteknek joguk van ahhoz is, hogy hozzáférjenek az ezeken a biometrikus adatokon alapuló lehetséges profilokhoz. Ha az adatkezelőnek az ilyen hozzáférés engedélyezése érdekében meg kell bizonyosodnia az érintettek személyazonosságáról, akkor elengedhetetlen, hogy az ilyen hozzáférést további személyes adatok feldolgozása nélkül biztosítsák.

3.6. Adatbiztonság

Az adatkezelőknek megfelelő technikai és szervezeti intézkedéseket kell végrehajtaniuk a személyes adatoknak a véletlen vagy jogellenes megsemmisülés, véletlen elvesztés, megváltoztatás, jogosulatlan közlés vagy hozzáférés, illetve a feldolgozás minden más jogellenes formája elleni védelme érdekében[9].

Az összegyűjtött és tárolt adatok biztonságáról megfelelően kell gondoskodni. A rendszerek tervezőinek megfelelő biztonsági szakértőket kell bevonniuk annak biztosítása érdekében, hogy megfelelően kezeljék a gyenge biztonsági pontokat, különösen, ha a meglévő rendszereket az internetre telepítik.

3.7. A sajátos igényű személyekre vonatkozó biztosítékok

A biometria használata jelentős hatást gyakorolhat a kiszolgáltatott személyek – például a fiatal gyermekek, az idősek és az adatfelvételi folyamat sikeres elvégzésére fizikailag képtelen személyek – méltóságára, magánéletére és adatvédelemhez való jogára. Az érintett személyekre vonatkozó potenciálisan káros következményekre tekintettel a szükségesség és arányosság megkérdőjelezését, valamint az egyénnek az adatvédelemhez fűződő joga gyakorlására vonatkozó lehetőségeit illetően szigorúbb követelményeknek kell megfelelni az egyének méltóságába beavatkozó intézkedésekhez kapcsolódó hatásvizsgálati folyamat során ahhoz, hogy az adott intézkedés elfogadhatónak minősüljön. Megfelelő biztosítékokat kell bevezetni annak kockázata ellen, hogy ezeket a személyeket a koruk vagy az adatfelvételre való képtelenségük miatt megbélyegezzék vagy megkülönböztessék.

Azt illetően, hogy általános jogi kötelezettség legyen-e a biometrikus azonosítók gyűjtése e csoportokra vonatkozóan, elsősorban a fiatal gyermekek és idősebb személyek határellenőrzés során történő azonosítása céljából, a munkacsoport azt az álláspontot vallja, hogy *„a*

[9] A 95/46/EK irányelv 17. cikkének (1) bekezdése.

személyek méltóságának tiszteletben tartása és az eljárás megbízhatósága érdekében a gyermekek és idősebb személyek esetében korlátozni kell az ujjlenyomatok begyűjtését és feldolgozását, és a korhatárnak összhangban kell lennie az egyéb nagy uniós biometrikus adatbázisok (különösen az Eurodac) vonatkozásában alkalmazott korhatárokkal."[10]

Mindenesetre különleges biztosítékokat (mint amilyenek a megfelelő tartalékeljárások) kell bevezetni annak érdekében, hogy biztosított legyen a felvételi folyamatot sikeresen elvégezni képtelen egyének emberi méltóságának és alapvető szabadságainak tiszteletben tartása, és ilyen módon ne terheljék az ilyen egyéneket a technikai rendszer tökéletlenségei[11].

3.8. Különleges adatok

Egyes biometrikus, különösen a faji vagy etnikai származást felfedő vagy az egészségre vonatkozó adatok a 95/46/EK irányelv 8. cikkének értelmében különlegesnek tekinthetők. A személyek DNS-adatai például gyakran tartalmaznak egészségügyi adatokat, illetve felfedhetik a faji vagy etnikai származást. Ebben az esetben a DNS-adatok különleges adatok, és az irányelv általános adatvédelmi elvein túl a 8. cikkben előírt speciális biztosítékokat is alkalmazni kell. Egy adott biometrikus rendszer által feldolgozott adatok különleges voltának megítélése érdekében figyelembe kell venni a feldolgozás körülményeit is[12].

3.9. A nemzeti adatvédelmi hatóságok szerepe

Figyelemmel arra, hogy az átjárhatóság érdekében egyre szélesebb körű a biometrikus technológiák szabványosítása, általánosan elfogadott, hogy a biometrikus adatok központosított tárolása megnöveli mind annak a kockázatát, hogy a biometrikus adatokat kulcsként használják több adatbázis összekapcsolásához (ami azt eredményezheti, hogy részletes profilt hoznak létre az egyénről), mind az ilyen adatok nem megfelelő célokra való újbóli felhasználásának sajátos veszélyeit, különösen engedély nélküli hozzáférés esetében.

A munkacsoport azt javasolja, hogy azokhoz a rendszerekhez, amelyek biometrikus adatokat használnak kulcsként több adatbázis összekapcsolásához, további biztosítékok legyenek szükségesek, mivel az ilyen típusú feldolgozás valószínű, hogy külön kockázatot jelent az érintettek jogaira és szabadságaira nézve (a 95/46/EK irányelv 20. cikke). Annak érdekében, hogy az adatkezelő megfelelő biztosítékokról gondoskodjon, és különösen, hogy csökkentse az érintettekre vonatkozó kockázatokat, konzultálnia kell a hatáskörrel rendelkező nemzeti adatvédelmi hatósággal az ilyen intézkedések bevezetése előtt.

---

[10] WP 134; 3/2007. sz. vélemény a diplomáciai és konzuli képviseletek számára kibocsátott, a vízumokra vonatkozó Közös Konzuli Utasításnak a biometrikus adatok bevezetésével, valamint a vízumkérelmek fogadása és feldolgozása megszervezésének rendelkezéseivel kapcsolatos módosításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (COM(2006) 269 végleges).

[11] Vö. WP134; 3/2007. sz. vélemény, 8. o.

[12] Vö. WP 29. sz. tanácsadó dokumentum az adatok különleges kategóriáiról („különleges adatok"), Ref. Ares (2011)444105 – 2011.4.20.

4. Új fejlemények és technológiai trendek, új forgatókönyvek

4.1. Bevezetés

A biometrikus technológiákat már régóta használják, főként a kormányzati hatóságok, de a közelmúltban a helyzet fokozatosan átalakult, mára a kereskedelmi szervezetek elsődleges szerepet játszanak e technológiák használata és az új termékek kifejlesztése terén.

Az egyik kulcsszerepet játszó tényező e helyzet kialakulásában az, hogy a technológia kiforrottabbá vált, azok a biometrikus rendszerek, amelyek korábban csak ellenőrzött körülmények között működtek jól, kifinomultabbá váltak, és most már alkalmasak arra, hogy szélesebb körben, sokféle különböző környezetben használják őket. Ilyen értelemben a biometrikus technológiák egyes esetekben felváltják vagy javítják a hagyományos azonosítási módszereket, különösen azokat, amelyek a stabil hitelesítési rendszerekhez szükséges többféle azonosító tényezőn alapulnak. A biometrikus technológiákat egyre nagyobb mértékben használják olyan alkalmazásokban is, amelyek gyorsan és kényelmesen, azonban alacsonyabb pontossággal képesek az azonosításra.

A biometrikus technológiák alkalmazása fokozatosan kiterjed az eredeti alkalmazási körhöz képest is: az azonosításról és hitelesítésről a viselkedéselemzésre, a felügyeletre és a csalásmegelőzésre.

A számítógépes technológiák és hálózatok terén történt előrelépések is azon technológiák felemelkedéséhez vezetnek, amelyeket második generációs biometrikus technológiáknak tekintenek, ezek vagy kizárólag viselkedési és pszichológiai vonások használatán alapulnak, vagy más, klasszikus rendszerekkel kombinálva multimodális rendszereket képeznek. Hogy teljes legyen a kép, a biometriát egyre szélesebb körben használják a környezeti intelligencia és a helyfüggetlen számítástechnika fejleményei terén.

4.2. A biometriára vonatkozó új trendek

Több olyan biometrikus technológia létezik, amelyet kiforrott technológiának lehet tekinteni, és számos alkalmazása van a bűnüldözés, az e-kormányzat és a kereskedelmi rendszerek terén. A teljesség igénye nélkül ide tartoznak az ujjlenyomatok, a kézgeometria, az íriszszkennelés és az arcfelismerés egyes típusai. Terjedőben vannak a test jellemzőinek elemzésén alapuló egyes biometrikus technológiák is. Míg ezek közül néhány új, egyes hagyományos biometrikus technológiák is új lendületet kapnak az új feldolgozási kapacitásoktól.

Ezeknek az új rendszereknek tipikus eleme a test olyan jellemzőinek felhasználása, amelyek lehetővé teszik az egyének kategorizálását/azonosítását, valamint az ilyen jellemzők távolról történő gyűjtése. Az összegyűjtött adatokat profilalkotásra, távfelügyeletre vagy akár olyan összetettebb feladatokra használják, mint amilyen a környezeti intelligencia.

Ez azért vált lehetővé, mert folyamatosan fejlődtek az érzékelők, ami lehetővé tette új fizikai jellemzők gyűjtését és a hagyományos biometrikus adatok új feldolgozási módjait.

Meg kell említeni az úgynevezett másodlagos biometria alkalmazását is, amely az egyének egyértelmű megkülönböztetésére vagy azonosítására nem alkalmas, de más azonosító rendszerek teljesítményének fokozását lehetővé tevő nagyon általános vonások használata határoz meg.

Az új biometrikus rendszerek egy másik alapvető eleme annak lehetősége, hogy távolról vagy mozgás közben gyűjtsenek információkat, anélkül, hogy ahhoz szükséges lenne az egyén

együttműködése vagy cselekvése. Bár maga a technológia még nem teljesen kidolgozott, jelentős előrelépésekre kerül sor e téren, különösen bűnüldözési célokból.

Gyorsan terjed az egyszerre különböző biometrikus adatokat használó vagy ugyanazon biometrikus adatok többszöri / több egységének leolvasásán alapuló multimodális rendszerek használata, amelyek a biometrikus rendszerek biztonságának / kényelmes alkalmazásának optimalizálása érdekében kiigazíthatók. Ez csökkentheti a hibás elfogadási arányt, javíthatja egy adott felismerőrendszer eredményeit, vagy megkönnyítheti egy nagyobb populáció adatainak gyűjtését azzal, hogy a biometrikus adatok egy bizonyos forrásának nem univerzális jellegét kiegyensúlyozza egy másik adatforrással való összekapcsolással.

A biometrikus rendszereket egyre nagyobb mértékben használják mind a köz-, mind a magánintézmények; a közszférában hagyományosan a bűnüldözés terén használnak rendszeresen biometrikus adatokat; a pénzügyi, banki és e-egészségügyi ágazatban gyorsan terjed a biometrikus technológiák használata, ugyanúgy, mint más ágazatokban, például az oktatásban, a kiskereskedelemben és a hírközlésben. Ezt a fejlődést a meglévő technológiák konvergenciájából/fúziójából eredő újítások hajtják majd előre. Az egyik példa a CCTV-rendszerek használata, amelyek lehetővé teszik a biometrikus adatok és emberi viselkedési jellemzők gyűjtését és elemzését is.

A fentiek értelmezhetők olyan módon is, hogy megváltozik a biometrikus rendszerek fejlődésének fókusza, az azonosító eszközök helyett már a „másodlagos" felismerési célok állnak a középpontban, más szóval az azonosításról a viselkedésre vagy az emberek speciális igényeinek felismerésére kerül a hangsúly. Ez megnyitja az utat a nagy léptékű biztonsági alkalmazásoktól merőben eltérő felhasználások előtt is: a személyes biztonság, a játék és a kiskereskedelem is profitálni fog az ember és gép közötti javuló interakcióból, amely többet tesz lehetővé az egyének azonosításnál vagy kategorizálásánál.

4.3. A magánélet védelmére és az adatvédelemre gyakorolt hatás

A biometrikus rendszerekről már a bevezetésük kezdetétől fogva elismerték, hogy számos területen súlyos aggodalmakat vethetnek fel, ideértve a magánélet védelmét és az adatvédelmet. Ez bizonyosan befolyásolta az ilyen rendszerek társadalmi elfogadottságát, és felélénkítette a jogszerűségükről és a használatuk korlátairól, valamint az azonosított kockázatok enyhítése érdekében szükséges biztosítékokról és garanciákról folyó vitát.

A biometrikus rendszerekkel szembeni hagyományos ellenállás az egyéni jogok védelméhez kapcsolódott, és ez továbbra is így van. Az új rendszerek és a meglévő rendszerek fejlesztései mindazonáltal számos aggodalmat vetnek fel. Ezek közé tartozik a leplezett adatgyűjtés, adattárolás és adatfeldolgozás lehetősége, valamint a rendkívül különleges információkat tartalmazó anyagok gyűjtése, ami az egyén legintimebb szférájába törhet be.

A funkciók bővülése miatt már a biometrikus technológiák és rendszerek első alkalmazásától kezdve komolyan aggódtak; bár ez egy jól ismert és kezelt kockázat a hagyományos biometria terén, kétségtelenül egyértelmű, hogy az új számítógépes rendszerek magasabb technikai potenciálja fokozza annak kockázatát, hogy az adatokat az eredeti céljukkal ellentétes módon használják fel.

A leplezett technikák lehetővé teszik az egyének tudtukon kívüli azonosítását, ami a magánéletet érintő súlyos fenyegetést eredményez, és csökkenti a személyes adatok feletti ellenőrzést. Ez súlyos következményekkel jár az egyének azon képességére, amelynek értelmében önkéntes hozzájárulást adhatnak vagy egyszerűen csak tájékozódhatnak a feldolgozásról. Ezenkívül egyes rendszerek titokban az érzelmi állapothoz vagy testi

jellemzőkhöz kapcsolódó adatokat gyűjthetnek és egészségügyi adatokat fedhetnek fel, ami aránytalan adatfeldolgozást, illetve a 95/46/EK irányelv 8. cikkének értelmében vett különleges adatok feldolgozását eredményezi.

Figyelembe véve azt a tényt, hogy a biometrikus technológiák nem képesek teljes pontosságot biztosítani, mindig fennáll a helytelen azonosításból eredő kockázat. Az ilyen hamis pozitív azonosítások az egyéni jogokat érintő döntéseket eredményeznek. A csalással előállított vagy lopott biometrikus adatok használatán alapuló személyazonosság-lopás súlyos károkhoz vezethet. Más azonosító rendszerektől eltérően nem lehet egyszerűen új azonosítót biztosítani valakinek csak amiatt, mert az eredeti veszélybe került.

Meg kell említeni a profilalkotást is az automatizált döntések kapcsán, vagy egy bizonyos helyzetben tanúsított viselkedés vagy mutatott preferenciák előrejelzéséhez kapcsolódóan. Egyes biometrikus adatok fizikai információkat fedhetnek fel az egyénről. Ez felhasználható célzott tevékenységek és profilalkotás céljára, de eredményezhet megkülönböztetést, megbélyegzést vagy váratlan/nemkívánatos információkkal való akaratlan szembesülést is.

4.4. Konkrét biometrikus rendszerek és technológiák

4.4.1. Érmintázat és kombinált felhasználás

Két fő használatban lévő technológia alapul érmintázat-felismerésen: a tenyér érmintázatának felismerése és az ujj érmintázatának felismerése, ma már mindkét technológiát széles körben használják, különösen Japánban.

Az érmintázat-felismerés technikailag az erek sablonján alapul, amelyet infravörös kamera rögzít, miközben az ujjat infravöröshöz közeli fény világítja meg. A rögzített képet feldolgozzák, hogy kirajzolódjanak az érmintázat jellegzetességei, ami az érhálózat utómunkával módosított képét eredményezi. E technológia fő előnye abban rejlik, hogy nem hagyja ott minden egyes személy a biometrikus jellemzőinek a nyomát[13], mivel nem kell megérinteni a leolvasót. Emellett jelenleg nehéz a biometrikus adatoknak az érintett hozzájárulása nélküli gyűjtése. Végül pedig ez a technika a vér áramlásának vizsgálata útján annak észlelésére is használható, hogy a rendszernek bemutatott alany életben van-e vagy sem.

Az érmintázat-felismerés felhasználható logikus hozzáférési alkalmazások és helyiségekhez való fizikai hozzáférés céljára. A gyártók felkínálják annak lehetőségét is, hogy az érzékelőt beépítsék más, főként banki célra használt termékekbe.

Az érmintázaton alapuló rendszerek használatával összefüggő adatvédelmi kockázatok a következőképpen írhatók le:

- Pontosság: az érmintázat-felismerés teljesítményszintje magas, mivel ezt a technológiát az ujjlenyomatok használatának lehetséges alternatívájának tekintik. Az érmintázat-felismerés esetén alacsony az adatfelvételi hibák aránya is (Failure to Enrol Rate, FER), mivel ezt a technológiát nem befolyásolja az ujj vagy a kéz állapotának romlása. Ezekkel a technológiákkal még nem kísérleteztek / nem használták őket nagyon nagy populációban (Japánban a

[13] Egyes szerzők azt állítják, hogy az érmintázat-felismeréshez kapcsolódó technológiák felfedhetnek olyan betegségeket, mint a magas vérnyomás vagy az érrendszeri rendellenességek.

sablont az intelligens kártyán tárolt sablonnal hasonlítják össze). Ezt a technológiát egyes esetekben befolyásolhatják a környezeti körülmények is, amelyek hatást gyakorolnak az érrendszerre (hőhatás, nyomás stb.).

- Hatás: az érmintázaton alapuló rendszerek csak kismértékben gyakorolnak hatást az adatvédelemre, mivel a biometrikus adatok gyűjtése nem egyszerű, és az érmintázatot jelenleg csak magánszektorbeli alkalmazásokban használják.

- Hozzájárulás és áttekinthetőség: mivel az érmintázatra vonatkozó adatok csak infravöröshöz közeli megvilágítás és kamerák használatával gyűjthetők, a személy vélhetően tudatában van az adatfeldolgozásnak és hozzájárulását adja azzal, hogy a leolvasóra helyezi az ujját vagy a kezét. Azonban – mint bármely más biometrikus rendszer esetében – ezt a vélelmet egyes sajátos helyzetekben enyhíteni kell, például ha a személy az adatkezelő alkalmazottja.

- A feldolgozás további célja vagy céljai: jelenleg az érmintázatra vonatkozó adatok korlátozott mértékben jelentenek kockázatot a további célra való felhasználást tekintve. Ez a kockázat növekedhet, ha általánossá válik az ilyen típusú feldolgozás, és ha könnyebbé válik a csalás.

- Összekapcsolhatóság: az érmintázatra vonatkozó adatok nem nyújtanak olyan információkat, amelyek összekapcsolhatók lennének más adatokkal, kivéve más feldolgozásból származó érmintázat-adatokat.

- Nyomon követés / profilalkotás: az érmintázat-adatok alapján való nyomon követés / profilalkotás kockázata alacsony, amíg nem használják széles körben az ilyen típusú biometriát, például a bankkártyák központi adatbázisában.

- Különleges adatok feldolgozása: az érmintázat-adatokból csak olyan különleges adatok származtathatók, amelyek az egészségügyi állapotra vonatkoznak, de ebben a témában még nem végeztek hivatalos vizsgálatot.

- Megmásíthatóság: úgy tűnik, az érmintázatra vonatkozó adatok időben kifejezetten állandók, de ezt kísérleti úton kell megerősíteni (az érmintázathoz kapcsolódó rendszerek még túl újak ahhoz, hogy alátámasztott eredményeket adjanak). Az érmintázat-adatokat tehát megmásíthatatlannak kell tekinteni.

- Csalás elleni védelem: az érmintázat-adatok csalással való előállítását még nem tárták fel kimerítően, de egy közelmúltbeli kutatás szerint lehetséges megtéveszteni a tenyérerezet-olvasókat[14]. Az érmintázat-adatok csalással való előállítása terén a legfőbb nehézség a biometrikus adatok mintájának megszerzése.

4.4.2. Ujjlenyomatok és kombinált felhasználás

Az ujjlenyomat-felismerés a legrégebbi és legszélesebb körben tanulmányozott, leginkább használt biometrikus rendszerek közé tartozik. Az ujjlenyomat alapján történő azonosítást már több mint 100 éve használják a bűnüldözés terén mind ellenőrzési, mind azonosítási feladatokra. Azon a tényen alapul, hogy mindenki egyedi ujjlenyomatokkal rendelkezik,

[14] Lásd: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

amelyek olyan sajátos jellemzőket mutatnak, amelyek megmérhetők annak eldöntése érdekében, hogy az adott ujjlenyomat megfelel-e a felvett mintának.

A felvételhez szükséges az egyén fizikai jelenléte, és – a várható felhasználástól függően – jól képzett személyzetre is szükség van az adatok jó minőségének biztosítása érdekében. Az ujjlenyomat-rögzítés nem egyszerű feladat. Ebben az értelemben a megfeleltetés pontossága a képalkotási technikához képest a képminőségtől függ. A technikák változatosak, egy-két ujjtól mind a tíz ujj nyomatának lapos felületen vagy görgetett módon való levételéig terjednek. A rendszertől függően az ujjlenyomatok használhatók csak ellenőrzésre (1:1) vagy azonosításra és nyomoknak való megfeleltetésre (1:n). Ahogyan azonban néhány tanulmányból kiderült, a populáció egy része különböző okokból nem képes ujjlenyomatot adni, és ez olyan problémát jelent, amelyhez megfelelő tartalékeljárások megléte szükséges – különösen nagy rendszerek esetében –, hogy elkerüljék, hogy az egyéneket megfosszák olyasmitől, amire jogosultak.

Bár elméletileg nem túlzottan beavatkozó jellegű módszerről van szó, mégis ezt a benyomást keltheti, mivel a bűnüldözés terén való elterjedt használata miatt az a kedvezőtlen kép alakulhat ki az egyénben, hogy gyanúsítottként kezelik.

Az ujjlenyomatok különböző jellemzőket mutatnak, amelyek felhasználhatók ellenőrzési/azonosítási célokra, bár továbbra is az apró részletek elemzése a leginkább használt technika. Az új technikák (vagyis a nagy felbontású szkennerek) fejlesztése lehetővé fogja tenni más jellemzők használatát is. Tovább fejlődtek a technikák az azonosítási képességet tekintve is, ami lehetővé tette a nagy adatbázisok azonosítási célú használatát.

Ebben az értelemben a legfejlettebb rendszerek a bűnüldözési célokra használt úgynevezett automata ujjlenyomat-azonosító rendszerek (AFIS), amelyek határok túloldalán elhelyezkedő különböző adattárakban való keresés útján adatmegosztásra használhatók. Az adatcsere a különböző helyszínekhez, formátumokhoz és színvonalhoz kapcsolódó problémákba ütközik.

Uniós szintű példa az AFIS-ra az Eurodac és a vízuminformációs rendszer, amelyek a várakozások szerint a világ legnagyobb adatbázisai közé fognak tartoznak majd, tekintve, hogy körülbelül 70 millió ujjlenyomatot fognak tárolni ezekben a rendszerekben. A munkacsoport korábbi véleményeiben számos kérdést vetett fel a nagyméretű adatbázisok használatára vonatkozóan, figyelemmel arra, hogy biztosítani kell az arányosságot. Különösen a hamis pozitív és hamis negatív megállapításokhoz kapcsolódó megbízhatósági problémákat, az ezekhez az adatbázisokhoz való hozzáférés hatékony ellenőrzését, valamint a gyermekek és idősek ujjlenyomatainak használatához kapcsolódó problémákat kell kezelni.

A sablonok ujjlenyomatvételen alapuló biometrikus rendszerekben való használata elterjedt, ezeket a rendszer-üzemeltetők általában az egyén védelme egy módjának tekintik. Mindazonáltal a sablon generálásához használt rendszertől/algoritmustól függően vannak olyan potenciális kockázatok, amelyek a sablonoknak más ujjlenyomat-adatbázisokhoz való, egyének azonosítását célzó hozzákapcsolásához köthetők.

Szintén fontos probléma az olyan rendszerek használata, amelyek az ujjlenyomat-felismerő rendszerek mesterséges ujjak vagy mesterséges anyagból készült ujjlenyomatok használatával való kijátszását szolgálják, és amelyek lehetővé teszik a személyazonosság-lopáshoz kapcsolódó gyakorlatokat. Különböző megoldások vannak a rendszerek sebezhetőségének csökkentésére, ilyenek az élő felismerés, a több ujj felismerésén alapuló rendszerek, illetve a felvételi és az azonosítási/ellenőrzési tevékenységek során való megfelelő emberi ellenőrzés.

Az ujjlenyomatok használatával kapcsolatban vannak adatvédelmi aggályok, ezek röviden a következőképpen írhatók le:

- Pontosság: bár az ujjlenyomatok végső soron nagy pontossági arányt eredményeznek, ez az információkhoz kapcsolódó korlátok – a rossz adatminőség vagy a nem következetes adatszerzési folyamat – vagy a megjelenítés korlátai, a kiválasztott jellemzők vagy a kinyerési algoritmusok minősége, miatt támadható. Ez téves elutasítást vagy téves megfeleltetéseket eredményezhet.

- Hatás: a folyamat visszafordíthatatlansága csökkentheti az egyén azon lehetőségét, hogy gyakorolja a jogait vagy megváltoztassa a hamis azonosítás alapján meghozott döntéseket. Az ujjlenyomatok használatának pontosságába vetett bizalom megnehezítheti a lehetséges hibák orvoslását, ami messze ható következményekhez vezet az egyénekre nézve. Ezt figyelembe kell venni a feldolgozásnak az ujjlenyomatok alapján meghozandó konkrét határozathoz viszonyított arányosságának értékelése során. Meg kell említeni azt is, hogy a biztonsági intézkedések hiánya személyazonosság-lopáshoz vezethet, amely jelentős hatással lehet az egyénre.

- Összekapcsolhatóság: az ujjlenyomatok lehetőséget nyújtanak a visszaélésre, mivel az adatok összekapcsolhatók más adatbázisokkal. A más adatbázisokkal való összekapcsolás e lehetősége az eredeti célokkal össze nem egyeztethető felhasználást eredményezhet. Vannak olyan technikák, mint az átváltható biometria vagy a biometrikus titkosítás, amelyeket fel lehet használni a kockázat csökkentése érdekében.

- Különleges adatok feldolgozása: néhány tanulmány szerint az ujjlenyomatok képei az egyénre vonatkozó etnikai információkat fedhetnek fel[15].

- A feldolgozás további célja vagy céljai: Az adatok központi tárolása – különösen nagy adatbázisokban – az adatbiztonsághoz, az összekapcsolhatósághoz és a funkciók terjeszkedéséhez kapcsolódó kockázatokkal jár. Ez biztosítékok hiányában lehetővé teszi az ujjlenyomatok olyan célokra való felhasználását, amelyek eltérnek a feldolgozást eredetileg indokoló céloktól.

- Hozzájárulás és átláthatóság: a hozzájárulás központi kérdés az ujjlenyomatok bűnüldözés területén kívül eső felhasználása terén. Az ujjlenyomatok könnyen lemásolhatók rejtett lenyomatokról vagy akár fényképekről is az egyén tudomása nélkül. A hozzájárulással kapcsolatos egyéb problémák a gyermek hozzájárulásának megszerzéséhez és a szülők e téren játszott szerepéhez (például iskolákban történő ujjlenyomatvétel kapcsán), valamint a munkaviszony keretében történő ujjlenyomat-vételhez való hozzájárulás érvényességéhez kapcsolódnak.

- Megmásíthatóság: az ujjlenyomat-adatok időben kifejezetten állandók, és megmásíthatatlannak tekintendők. Ujjlenyomat-sablon bizonyos feltételekkel megmásítható.

- Csalás elleni védelem: az ujjlenyomatok könnyen gyűjthetők, mert egy egyén több ujjlenyomatot hagy hátra. Ráadásul a hamis ujjlenyomatok sok rendszer és érzékelő

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm és http://www.crime-scene-investigator.net/fingerprintpatterns.html.

esetében felhasználhatók, különösen, ha az ilyen rendszereknek nem képezi részét külön csalás elleni védelem. A támadás sikere nagyrészt az érzékelő típusán (optikai, kapacitív stb.) és a támadó által használt anyagon múlik.

Példa:
Egy kórház központi adatbázisban tárolt ujjlenyomatokat használ arra, hogy sugárterápiás szolgáltatáshoz kapcsolódóan hitelesítse a betegeket annak biztosítása érdekében, hogy a beteg a megfelelő kezelést kapja. Az ujjlenyomatokat részesítik előnyben az érmintázat helyett, mert a kezelés károsítja az érrendszert. Azért használnak központi adatbázist, mert a betegek állapota (kor, betegségek) miatt magas annak a kockázata, hogy elveszítsék a belépőkártyákat, ami megakadályozná a kezeléshez való hozzáférést. Ebben az esetben az ujjlenyomatok használata megfelelő megoldásnak tűnik.

4.4.3. Arcfelismerés és kombinált felhasználás

Az ujjlenyomatokhoz hasonlóan az arcot is több éve használják széles körben a biometrikus adatok forrásaként. Újabban már nemcsak a személyazonosság állapítható meg az arc alapján, hanem olyan fiziológiai és pszichológiai jellemzők is, mint az etnikai származás, az érzelmek és a jóllét. Az, hogy egy képből ilyen mennyiségű információt lehet kinyerni, és az a tény, hogy az érintettről bizonyos távolságból, a tudtán kívül is lehet fényképet készíteni, jól jelzi, mennyi adatvédelmi probléma eredhet az ilyen technológiákból.

Az arcfelismerésre mint azonosítási és ellenőrzési módszerre felfigyeltek a bűnüldöző szervek, más hatóságok és még a magánszervezetek is. A fényképek már sok éve megjelennek az útlevelekben, vezetői engedélyekben, nemzeti személyazonosító igazolványokban és a bűnügyi nyilvántartásban. Nem ritka az sem, hogy belépőkártyára vagy más szervezeti azonosítókártyára nyomtatnak fényképet. Ezeket a fényképeket általában szabályozott világítás mellett készítik el, és csak az egyén szemből vagy profilból látható képét tartalmazzák. Az ilyen szabályozott képkészletek használata kézenfekvőnek bizonyult az automatikus feldolgozás és az egyének automatikus felismerésének a megkezdésére. Ez a képesség azóta már túlhaladott, és a technológia ott jár, hogy többféle fényképezőgéppel, más-más nézőpontból és eltérő világítási körülmények között készült fénykép alapján is lehetséges az azonosítás. Hatalmas mennyiségű kép áll nyilvánosan rendelkezésre az interneten is, például a közösségi hálózatokra és más nyilvánosan elérhető galériákba felöltött képek. Az ilyesféle kockázatok nem korlátozódnak a hagyományos képekre, mivel az arcfelismerést sikeresen beépítették az élő videoközvetítésekbe is. Ha új feldolgozási képességgel ruháznak fel egy meglévő rendszert (például arcfelismerést építenek be egy CCTV-rendszerbe), akkor az adatkezelőknek fel kell ismerniük, hogy ez megváltoztathatja az eredeti rendszer meghatározott célját vagy céljait, és újra kell értékelniük a változás magánéletre gyakorolt hatását.

Az arcfelismerő rendszerek használatával összefüggő adatvédelmi kockázatok a következőképpen írhatók le:

- Pontosság: ha a képek minősége nem garantálható, akkor fennáll a kockázata annak, hogy sérül a pontosság. Ha nem rögzítik az arcot (azt haj vagy kalap takarja el), akkor egyértelmű, hogy csak magas hibaaránnyal kerülhet sor megfeleltetésre vagy kategorizálásra. A testtartás és a megvilágítás továbbra is nagy kihívást jelent az arcfelismerés terén, és nagymértékben befolyásolja a pontosságot.

- Hatás: egy adott arcfelismerő rendszer adatvédelemre gyakorolt konkrét hatása a rendszer rendeltetésétől és a sajátos körülményektől függ. Egy olyan kategorizáló rendszer, amely – rögzítési képesség nélkül – egy látványosság látogatóinak demográfiai adatait méri, más hatást gyakorol az adatvédelemre, mint egy olyan rendszer, amelyet a bűnüldöző szervek használnak fedett megfigyelésre a lehetséges bajkeverők azonosítása céljából.

- Hozzájárulás és átláthatóság: az egyik olyan adatvédelmi kockázat, amely nincs jelen sok más típusú biometrikus adatfeldolgozás esetén, az, hogy a képek rögzítésére és feldolgozására többféle nézőpontból, eltérő környezeti körülmények között és az érintett tudomása nélkül is sor kerülhet. A munkacsoport a hozzájárulás meghatározásáról szóló 15/2011. sz. véleményében kiemeli, hogy ahhoz, hogy a hozzájárulás jogalapot képezzen a feldolgozáshoz, előzetes tájékoztatáson alapuló hozzájárulásnak kell lennie. Ha az érintett nem tud a képek arcfelismerést célzó feldolgozásáról, akkor nem lehet előzetes tájékoztatáson alapuló hozzájárulásról beszélni. Még ha az érintett tud is arról, hogy kamera működik, lehetséges, hogy vizuális alapon nem lehet különbséget tenni egy élő vagy felvételeket rögzítő CCTV-rendszer és egy arcfelismerő rendszer számára képeket rögzítő lencse között.

- A feldolgozás további célja vagy céljai: az akár jogszerűen, akár jogellenesen történt rögzítést követően a digitális képek könnyen megoszthatók vagy lemásolhatók abból a célból, hogy az eredetileg szándékolttól eltérő rendszerekben dolgozzák fel őket. Ez nyilvánvaló a közösségi média esetében, ahol a felhasználók feltöltik a személyes fényképeiket, hogy megosszák azokat a családjukkal, a barátaikkal és a munkatársaikkal. Miután a képek bekerülnek a közösségi média platformjára, maga a platform számos célra újrafelhasználhatja a képeket, amelyek között lehetnek olyanok is, amelyeket a kép rögzítése, illetve feltöltése után vezetnek be a platformon.

- Összekapcsolhatóság: nagyon sok online szolgáltatás lehetővé teszi a felhasználók számára, hogy olyan képet töltsenek fel, amelyet összekapcsolnak a felhasználó profiljával. Az arcfelismerés felhasználható arra, hogy kapcsolatot hozzanak létre a különböző online szolgáltatások profiljai között (a profilkép útján), de akár az online és az offline világ között is. Nem elképzelhetetlen, hogy valakit lefényképezzenek az utcán, majd valós időben meghatározzák a személyazonosságát a nyilvános profilképek között végrehajtott kereséssel. Harmadik felek szolgáltatásai is átfésülhetik a profilképeket és más nyilvánosan elérhető fényképeket, hogy hatalmas képgyűjteményeket hozzanak létre annak érdekében, hogy egy valós személyazonosságot kapcsoljanak az ilyen képekhez.

- Nyomon követés / profilalkotás: akkor is használható azonosítórendszer, ha az egyén valós személyazonossága nem ismert. Bevásárlóközpontban vagy hasonló nyilvános területen telepített arcfelismerő rendszer használható lenne arra, hogy nyomon kövessék az egyes vásárlók útvonalát és szokásait. A célok szolgálhatnák a sorok hatékony kezelését vagy a termékelhelyezést a vásárlói élmény javítása érdekében. Ha valaki azonban képes egy adott egyén nyomon követésére vagy helyének meghatározására, akkor képes a profilalkotásra is, és képes célzott reklámozást vagy más különleges szolgáltatásokat nyújtani.

- Különleges adatok feldolgozása: a korábban említettek szerint a biometrikus adatok feldolgozása használható lenne különleges adatok megállapítására, különösen a látható

jelekkel járó adatokéra, mint amilyen a faj, az etnikai csoport vagy esetleg egy betegség.

- Megmásíthatóság: az egyének könnyen megváltoztathatják az arcuk kinézetét (szakáll, szemüveg, kalap stb.), ami elég lehet arra, hogy megtévesszék az arcfelismerő rendszereket, különösen, ha azok nem ellenőrzött környezetben működnek. Az egyének legfőbb arcvonásai azonban időben nem változnak, és a rendszerek is fejleszthetik a felismerést azzal, hogy az egyén különböző ismert „arcait" gyűjtik össze és kapcsolják az adott személyhez.

- Csalás elleni védelem: sok arcfelismerő rendszert egyszerű megtéveszteni, de a gyártók igyekeznek javítani a csalás elleni védelmet olyan technikák alkalmazásával, mint a háromdimenziós képalkotás vagy a videofelvételek. A nyilvános alkalmazásokban használt legtöbb kezdetleges rendszerben azonban nincs ilyen típusú védelem.

Példa:
Szélsőséges esetben előfordulhatna például az is, hogy egy bevásárlóközpont olyan következő generációs videomegfigyelési rendszerrel rendelkezik, amely képes felismerni a személyeket, automatikusan nyomon követni a mozgást, megkülönböztetni olyan jellemző arckifejezéseket, mint egy mosoly vagy a harag. Felismerhetné az épület parkolójába érkező törzsvásárlókat, és az általuk kedvelt parkolóhelyekhez irányíthatná őket. Amikor a vásárlók belépnek a bevásárlóközpontba, a rendszer azonosíthatná a ruháikat, hogy a boltok aktuális kínálatától, a korábbi vásárlásoktól vagy előre meghatározott mutatóktól függően javaslatot tegyen arra, hogy a vásárló mely boltokba látogasson el. Megoldható a személyre szabott reklámozás a kirakatokban, valamint a boltokba, éttermekbe és más helyekre való belépés automatikus megtagadása is. A potenciális autótolvajokat még azelőtt azonosítani lehetne és nyomon lehetne követni, mielőtt hozzáérnének egy autóhoz. Szükség esetén kamerával és más érzékelőkkel ellátott, távolról irányított légi eszközök (drónok) követhetnék nyomon a gyanús személyeket, amíg a gyanút el nem oszlatják vagy meg nem erősítik. Észlelni lehetne a ruházatban elrejtett tárgyakat (késeket vagy lopott cikkeket). Ez a technológia nem csak új biometrikus rendszereken alapul. Olyan információkat kombinál és dolgoz fel, amelyek különböző rendszerekből már rendelkezésre állnak más adatokkal együtt.

Hasonló alkalmazást terveztek az INDECT-projekt (városi környezetben a polgárok biztonságát szolgáló, megfigyelést, kutatást és felderítést támogató intelligens információs rendszer) részeként, amelyben a technológiákat annak érdekében kombinálják, hogy még a megtörténtük előtt megbirkózzanak a lehetséges terrorista cselekményekkel és bűncselekményekkel. A munkacsoport különösen hangsúlyozza, hogy a biometria ilyen használatához megfelelő jogalapra, valamint az ilyen intézkedések szükségességére és arányosságára vonatkozó szigorú mérlegelésre lenne szükség.

4.4.4. Hangfelismerés és kombinált felhasználás

A hangfelismerés azonosítási célú biometrikus technológiaként való használata mellett egy viszonylag elterjedt felhasználási mód esetén azonosítják a hangmintázaton belüli sajátos vonásokat a beszélő kategorizálása érdekében. Erre példa egy adott személy

telefonbeszélgetés során adott válaszainak az elemzése a stresszmintázatok és a rendellenes beszéd azonosítása céljából, hogy felismerjék a csalás lehetséges eseteit.

A gyártók által közzétett nyilatkozatok szerint ilyen technológia bevezetésével a pénzügyi szolgáltató vállalatok növelték a csalásfelismerési arányt, és gyorsabb szolgáltatás vált lehetővé a valós igények teljesítése kapcsán.

Kategorizálási rendszerben való használat esetén az adatvédelmi kockázatok némileg eltérnek a biometrikus azonosító rendszer kockázataitól, mivel nincs felvételi szakasz, és nincs szükség a biometrikus sablonok hosszú távú tárolására. Azonban ha telefonbeszélgetést rögzítenek, ahogyan erre a pénzügyi intézmények esetében gyakran sor kerül, megfelelő ellenőrzéseket kell bevezetni ezen adatok biztonságának garantálása érdekében.

- Pontosság: egy ilyen rendszer egyik adatvédelmi kockázata különösen a hibás pozitív és hibás negatív észlelési arányban rejlik, azaz hogy mennyi embert azonosítanak tévesen csalóként, vagy mennyi hamis igényt nem ismernek fel. Bár egy kategorizálási rendszer magasabb hibaarányt lehet képes elviselni, mint az ellenőrzési vagy az azonosító rendszerek, mégis megfelelő folyamatokat kell bevezetni annak érdekében, hogy időben megoldják a helytelenül kategorizált eseteket.

- Hozzájárulás és átláthatóság: lehet a magánéletet támogató megközelítést alkalmazni az ilyen technológiák esetében, például gondoskodni lehet annak biztosításáról, hogy a hívásokat szűrjék az alkalmasság szempontjából, az érintetteket pedig tájékoztassák az alkalmazott folyamatról. Egy esettanulmányban az egyéneket a kísérletre alkalmatlannak tekintették, ha nem angol volt az anyanyelvük, a hallásukat vagy gondolkodási képességüket érintő fogyatékosságban szenvedtek, vagy ha volt telefonhoz hozzáférésük. Az igénylők szabadon dönthettek arról, hogy nem vesznek részt a beszélgetésben, és hagyományos módon szolgáltatnak információkat, de a beszélgetésben részt venni nem kívánó vagy arra képtelen érintettek is részt vehettek egy ilyen rendszerben anélkül, hogy hátrányos helyzetbe kerültek volna.

- A feldolgozás további célja vagy céljai: míg e technológia alkalmazásakor a legtöbb esetben speciális infrastrukturális változásokat kellene végrehajtani, miközben a köz- és magánszféra konszolidálja az informatikai infrastruktúráját, hogy olyan technológiákat építsen be, mint az internetprotokollon keresztüli hangtovábbítás, a hangfelismerő technológiák integrálása egyszerűbbé válhat az adatkezelő adatvédelmi kötelezettségeinek megfelelő figyelembevétele nélkül.

- Megmásíthatóság: bár az egyének képesek szándékosan elváltoztatni a hangjukat, a hangmintázatok meglehetősen állandóak, és hatékonyak lehetnek az egyének egyedi azonosítása terén, különösen, ha az egyént nem tájékoztatják (és így nem érzi szükségét annak, hogy elváltoztassa a hangját).

- Csalás elleni védelem: a felvett hangokat fel lehet használni a hangfelismerő rendszerek megtévesztésére. A csalás elleni technikák közé tartoznak a kontextuális ismeretekre vonatkozó kérdések/válaszok (az aznapi dátumra való rákérdezés vagy ritka szavak elismételtetése).

4.4.5. DNS

A DNS-szekvenálásra és -megfeleltetésre használt eszközök fejlődése és a DNS-elemzéshez szükséges berendezések megfizethető áron való elérhetősége szükségessé teszi a biometriáról szóló korábbi munkadokumentum (WP 80) egyes feltevéseinek újragondolását.

A DNS-profilalkotási technológiák terén az egyik legnagyobb változás a DNS-szekvenálás és -megfeleltetés műveleteihez szükséges idő csökkenése. Az évek során a tudományos kutatás és a biotechnológiai fejlesztők által elért folyamatos fejlődés napokról órákra, sőt egy óra töredékére csökkentette a DNS-profil létrehozásához szükséges időt.

A DNS-alapú online szolgáltatások piacának hirtelen beindulása fenyegetést jelent az egyének adatvédelemhez való jogára nézve, különösen, ha a szolgáltatáshoz biometrikus minták és biometrikus adatok különböző országok (köztük az Unión kívüli országok) közötti átadása szükséges, ha több adatfeldolgozó van, vagy ha hiányoznak a genetikus vagy egészségügyi adatok feldolgozására vonatkozó megfelelő biztosítékok.

Nagyon valószínű, hogy a közeljövőben lehetséges lesz a valós idejű (vagy közel valós idejű) DNS-profilalkotás és mintamegfeleltetés hordozható eszközök használatával, ez lesz majd a kezdőpontja az olyan, DNS-alapú biometrikus azonosító/hitelesítési rendszerek fejlődésének, amelyek nagyobb pontossággal működnek, mint az ujjlenyomaton, hangon és arcfelismerésen alapuló hitelesítés.

A DNS-profilalkotás fejlődését elősegítette az is, hogy a kormányok, bírák és bűnüldöző hatóságok egyre jobban érdeklődnek a bűnügyi nyomozásra használható biotechnológiák iránt. A DNS-megfeleltetés megbízhatósága miatt, és mert DNS-mintát az érintett tudomása nélkül is lehet gyűjteni, az idők során számos tagállam létrehozta az elítélt személyekhez kapcsolódó és a bűncselekmények helyszínén talált DNS-profilok központosított adatbázisát, illetve kezdeményezte annak létrehozását.

2005 májusában hét tagállam aláírta a „Prümi Szerződés” néven ismert megállapodást a tagállamok közötti bűnügyi nyomozások és igazságszolgáltatás terén történő együttműködés információcsere útján való megerősítéséről. A megállapodás új alapokra helyezi az együttműködést, mivel bizonyos hozzáférési jogokat biztosít az aláíró feleknek a kizárólag a bűnüldözéshez kapcsolódó nemzeti DNS-adatbázisokhoz, az ujjlenyomat-adatokhoz, a személyes és nem személyes adatokhoz, valamint a gépjármű-nyilvántartási adatokhoz. Azóta több tagállam csatlakozott a szerződéshez, és a megállapodás legfontosabb elemeit belefoglalták a 2008/615/IB tanácsi határozatba.

Ebben a jogi keretben számos tagállam rendelkezik már vagy rendelkezik hamarosan működő nemzeti adatbankkal, amely az elítélt személyek DNS-profiljait és a bűncselekmények helyszínén talált bizonyítékokat tartalmazza, ez pedig felvet néhány aggályt ezzel a konkrét adatfeldolgozási móddal kapcsolatban.

A DNS-adatbankok létrehozásához kapcsolódó egyik legfőbb probléma az, hogy a DNS-mintákból (génhelyekből) származó genetikai adatok felfedhetnek – nem rögtön a gyűjtési szakasz során – az egészségi állapottal, a betegségekre való hajlammal vagy az etnikai származással kapcsolatos információkat. Ezért a DNS-adatbázisok létrehozása jelentős kockázatot jelent az emberi méltóságra és az alapvető jogokra nézve. Ezt a kockázatot a Tanács 2009/C 296/01. sz. állásfoglalásában mérlegelték. Vannak konkrét rendelkezések arról, hogy a DNS-elemzést olyan kromoszómarégiókra korlátozzák, amelyekről genetikai információ nem íródik át, azáltal, hogy olyan konkrét DNS-markereket használnak,

amelyekről nem ismert, hogy sajátos örökletes jellemzőkkel kapcsolatos információkat tartalmaznának (ezt nevezik ESS-nek, európai szabványkészletnek is).

Az a lehetőség azonban, hogy az egyik nemzeti DNS-adatbázisban szereplő valamely kinyert marker a jövőben valamilyen örökletes jellemzőt vagy egyéb különleges információt fedhet fel, a biológia terén történő fejlemények folyamatos figyelemmel kísérését teszi szükségessé, és az a következménye, hogy ebben a sajnálatos esetben az adatbázisban szereplő egyes információkat azonnal törölni kell. Ezenkívül mivel ezek a DNS-adatbázisok elítélt személyek profiljait gyűjtik össze, szigorúan korlátozni kell az adatok statisztikai elemzését, hogy ne történjen nemi vagy faji alapú profilalkotás.

Ami a rendőrségi és büntető igazságszolgáltatási célú DNS-adatbázisokat illeti, az Emberi Jogok Európai Bírósága kimondta, hogy egyértelműen meg kell különböztetni a gyanúsítottak, illetve a bűncselekmény miatt elítélt személyek személyes adatainak és genetikai profiljának feldolgozását[16].

Fennáll annak a lehetséges kockázata is, hogy a DNS-elemzés fel nem derített bűncselekményhez vagy elítélt személyekhez kapcsolódó családtagok vagy hozzátartozók azonosítására használható, mivel az adatbázisban a DNS-profilok kereshetők részleges markerek alapján vagy helyettesítő karakterek használatával is. Ez a funkció felveti a családra vonatkozó keresésből származó információk nyomon követésének következményeivel kapcsolatos problémát.

Megjegyzendő az is, hogy sajátos kockázatok kapcsolódnak a genom-adatkészletek kutatás terén történő használatához. A munkacsoport úgy véli, hogy a mintákhoz és az adatokhoz való hozzáférést szigorúan a kutatói közösségre kell korlátozni, és kizárólag csak kutatási célokból szabad engedélyezni; ezenkívül tisztázni kell, hogy a kutatási megállapításokat és eredményeket milyen körülmények között közlik az egyénekkel (figyelemmel az egyének tudatlansághoz való jogára is) vagy integrálják orvosi nyilvántartásokba.

A DNS biometrikus adatként való használatával összefüggő adatvédelmi kockázatok a következőképpen írhatók le:

- Pontosság: bár a DNS nagyon nagy szintű pontosságot nyújt, figyelembe kell venni, hogy ez a pontosság az elemzett markerek (génhelyek) számától függ. A tesztelőrendszereknek a legmagasabb szintű pontosságot kell biztosítaniuk.

- Hatás: a DNS használata az egyénre nézve rendkívül beavatkozó jellegűnek tekinthető. A genetikai adatok különleges információkat fedhetnek fel. Az adatok statisztikai elemzése felhasználható profilalkotásra is, és diszkriminatív hatást gyakorolhat az érintett személyekre.

- A feldolgozás további célja vagy céljai: az új technológiák egyre növekvő mennyiségű adatcserét tesznek lehetővé. Ezért egyértelműnek kell lennie, hogy ki férhet hozzá egy DNS-adatbázis információihoz. A családra vonatkozó keresés és a faji alapú célzott keresés olyan új technológiának tekinthetők, amelyek megkérdőjelezik a jelenleg rendelkezésre álló DNS-adatbázisokban való feldolgozás eredeti célját.

[16] Az EJEB S. és Marper kontra Egyesült Királyság ügyben 2008. december 4-én hozott ítélete (ügyszám: 30562/04. és 30566/04.), különösen annak 125. bekezdése.

- Hozzájárulás és átláthatóság: ma már kínálnak olyan szolgáltatásokat, amelyek során DNS-elemzést végeznek postai úton küldött biológiai mintákon (például nyál), az elemzés eredményét pedig az interneten teszik elérhetővé. A személyazonosság nem megfelelő ellenőrzése lehetővé teheti egyének vagy jogi személyek számára, hogy más egyénektől származó mintákat küldjenek be, és így másokra vonatkozó különleges személyes adatokhoz jussanak.

- Összekapcsolhatóság: a DNS-szekvenálás útján megszerezhető információk mennyisége és sokfélesége miatt a DNS sok lehetőséget kínál a visszaélésre, mivel a kinyert adatok könnyen összekapcsolhatók más adatbázisokkal, ami lehetővé teszi az egyénekre vonatkozó profilalkotást. A családra vonatkozó keresés lehetővé teszi a hozzátartozókhoz való kapcsolást is.

- Különleges adatok feldolgozása: a DNS felfedhet az egészségi állapothoz, betegségekre való hajlamhoz vagy az egyén etnikai származásához kapcsolódó információkat. Az adatminimalizálás elvének a releváns génhelyek kiválasztásakor való alkalmazása ezért rendkívül fontos. Sok mintából hosszabb időn át is kinyerhetők DNS-információk, ezért javasolt annak biztosítása, hogy a mintákhoz szigorúan csak engedéllyel rendelkező felhasználók férhessenek hozzá, engedélyezett felhasználás céljából.

- Megmásíthatóság: a DNS nem másítható meg.

- Csalás elleni védelem: a DNS-t eleve nagyon nehéz meghamisítani, azonban sok esetben nem nehéz mintát venni valaki DNS-éből (például haj) a tudomása nélkül.

4.4.6. Aláírás-biometria

Az aláírás-biometria a hagyományos biometrikus technológiák új felhasználási példájának tekinthető. Az aláírás-biometria olyan viselkedésalapú biometrikus technikák összessége, amelyek egy adott személynek a saját kezű aláírás dinamikájában kifejeződő viselkedését mérik. Míg a hagyományos aláírás-felismerés az aláírás vizuális képére vonatkozó statikus vagy geometrikus jellemzőknek (az aláírás kinézetének) elemzésén alapul, az aláírás-biometria az aláírás dinamikus jellemzőinek (az aláírás létrejöttének) elemzését jelenti, ezért ezeket a technikákat gyakran „dinamikus aláírásnak” nevezik.

Az aláírás-biometriai rendszerek (például egy digitalizáló táblagép) által mért tipikus dinamikus jellemzők a nyomás mértéke, az írás szöge, a toll sebessége és gyorsulása, a betűk formálása, az aláírás tollvonásainak iránya és más egyedi dinamikus vonások. E jellemzők a felhasználást és fontosságot tekintve gyártónként eltérnek, és általában érintésérzékelő eszközökkel rögzítik őket. Egyes aláírás-felismerő eszközök képesek az aláírás statikus vonásainak (vizuális kép) és dinamikus vonásainak (nyomás, szög, sebesség stb.) elemzését kombinálva elvégezni az ellenőrzést.

Az aláírás-biometria használatával összefüggő adatvédelmi kockázatok a következőképpen írhatók le:

- Pontosság: lehetséges, hogy az emberek nem mindig ugyanúgy írnak alá, így problémáik akadhatnak a felvételi folyamat során és a személyazonosságuk igazolásakor.

- Hatás: előfordulhat, hogy a viselkedési jellemzőkön, például az aláíráson alapuló biometrikus adatok nem egyediek az idő múlásával, és az érintett megváltoztathatja

azokat. Az aláírás változásai fiziológiai eredetűek is lehetnek, és megakadályozhatják a sikeres ellenőrzést, ami azt eredményezi, hogy alternatív eljárások szükségesek az egyének személyazonosságának ellenőrzéséhez.

- Csalás elleni védelem: míg egy hagyományos aláírás grafikus képét egy képzett személy fénymásolással vagy számítógépes grafikai szoftverrel könnyen tudja utánozni és hamisítani, a dinamikus aláírás biztonságosabb, mert az ellenőrzési folyamatban a dinamikus jellemzőket is ellenőrzik, amelyek összetettek és egyedien jellemzik a személyek kézírásának stílusát.

5. Általános iránymutatások, ágazatspecifikus ajánlások és technikai és szervezeti intézkedések.

Biometrikus rendszer bevezetéséhez számos résztvevő együttműködése szükséges:

- gyártók: biometrikus érzékelők tervezése és tesztelése, biometrikus technológiák teljesítményének meghatározása;
- integrátorok: a fogyasztónak eladott végtermék megtervezése: ők választják ki a biometrikus technológiát és határozzák meg részben a rendszer céljait (a megrendelők célcsoportjának kiválasztásával);
- viszonteladók: a végtermék fogyasztóknak való értékesítése; általában tájékoztatják a megrendelőt a teljesítményről, a kockázatokról és esetleg a jogi keretről;
- üzembe helyezők: a termék üzembe helyezése a megrendelő helyiségeiben;
- megrendelők: biometrikus rendszer vásárlására vonatkozó döntés meghozatala: meghatározzák a feldolgozás célját és módszereit, és ilyen módon adatkezelők;
- érintettek: a rendszer által használt biometrikus adatok szolgáltatása.

Egyes résztvevők a fent leírt feladatok közül egy, vagy egynél több feladatot is ellátnak. Minden szerep esetében fennáll a biometrikus rendszereknek a magánélet tiszteletben tartásával összeegyeztethető használatának biztosítása iránti felelősség: például az üzembe helyező nem vezethet be olyan biztonsági funkciót, amelyet az integrátor határozott meg.

5.1. Általános elvek

A biometrikus adatokat illetően a biztonságnak elsődleges fontosságúnak kell lennie, mivel a biometrikus adatok megmásíthatatlanok: ebből következően a biztonság biometrikus adatokat érintő megsértése veszélyezteti a biometrikus adatok azonosítóként való további biztonságos használatát, valamint az érintett személyek adatvédelemhez való jogát, amelynek kapcsán nincs lehetőség a sérelem hatásainak enyhítésére.

A kockázatok az ilyen adatokat használó alkalmazások számának növekedésével fokozódnak (különösen a biztonság megsértésének és a funkciók terjeszkedésének kockázata). Minél több biometrikus adatot használnak, annál valószínűbb, hogy sor kerül biometrikus adatok ellopására.

A munkacsoport elismeri a jelenlegi tendenciát, amely szerint távoli hozzáférést tesznek lehetővé a biometrikus rendszerekhez, például az interneten továbbított interfészek útján. Ez a tendencia egy sor új biztonsági problémát vet fel, amelyek közül sok már jól ismert az informatikai ágazatban. Egy ilyen rendszer bevezetésébe már a tervezés korai szakaszában megfelelő technikai biztonsági személyzetet kellene bevonni az informatikai ágazatból.

A munkacsoport a biometrikus adatok feldolgozásának magas szintű, a legújabb technikai lehetőségeket felhasználó technikai védelmét ajánlja. E tekintetben a munkacsoport ajánlja a

biometrikus információkat feldolgozó rendszerek védelmét szolgáló ágazati szabványok követését.

5.2. Beépített adatvédelem

A beépített adatvédelem azt jelenti, hogy az adatvédelmet eleve magába a technológiába beépítik.

Ami a biometrikus rendszereket illeti, a beépített adatvédelem a biometrikus rendszerek teljes értékláncára vonatkozik:

- A gyártóknak az új technológiák és érzékelők tervezésekor végre kell hajtaniuk a beépített adatvédelem elveit: ide tartozhat a nyers adatok automatikus törlése a sablon kiszámítása után, vagy a titkosítás használata a biometrikus adatok tárolása terén (akár központi adatbázisban, akár intelligens kártyán történik a tárolás). A gyártóknak emellett olyan biometrikus technológiák kifejlesztésére kell összpontosítaniuk, amelyek biztosítják a magánélet védelmét.
- Az integrátoroknak és a viszonteladóknak is meg kellene valósítaniuk a beépített adatvédelem elveit az értékesítendő végtermék meghatározásakor azáltal, hogy a magánéletet védő technológiákat választanak, és olyan biztonsági intézkedéseket építenek be a végtermékbe, amilyen például az adatbázis decentralizációja.
- A megrendelőknek (leendő adatkezelőknek) a biometrikus rendszer igényelése vagy a rendszer technikai jellemzőinek meghatározása során alkalmazniuk kellene a beépített adatvédelem elveit. Ebben az esetben a gyártóknak és integrátoroknak bizonyos szintű rugalmasságot kellene biztosítaniuk a terméküket illetően, hogy teljesüljön az arányosság, a célhoz kötöttség, az adatminimalizálás és a biztonság elve.

Ezeket az elveket már sikeresen megvalósították egyes biometrikus eszközökben: néhány gyártó titkosítási funkciókkal, illetve leszerelés és rongálás esetén jelző riasztókkal látott el egyes biometrikus leolvasókat, hogy megakadályozza a biometrikus adatokhoz való engedély nélküli hozzáférést.

A munkacsoport azt ajánlja, hogy a biometrikus rendszereket hivatalos „fejlesztési ciklusok” alapján tervezzék, amelyeknek a következő lépések képezik részét:

1. a követelmények meghatározása kockázatelemzés, illetve külön magánélet-védelmi hatásvizsgálat alapján;
2. annak leírása és indokolása, hogy a kialakítás megfelel a követelményeknek;
3. működési és biztonsági tesztekkel való validálás;
4. annak ellenőrzése, hogy a végső kialakítás megfelel-e a szabályozási keretnek.

A munkacsoport ösztönzi olyan tanúsítási rendszerek meghatározását, amelyek biztosíthatnák a beépített adatvédelem megvalósítását és növelhetnék az adatkezelőknek a biometrikus rendszerekhez kapcsolódó adatvédelmi kockázatokról való tájékoztatását.

5.3. A magánélet-védelmi hatásvizsgálat kerete

5.3.1. Általános elvek

A magánélet-védelmi hatásvizsgálat olyan folyamat, amelynek során a szóban forgó jogalany elvégzi a személyes adatok feldolgozásához kapcsolódó kockázatok elemzését, és meghatározza az e kockázatok enyhítését célzó további intézkedéseket. Az RFID-technológia esetében a munkacsoport megállapította, hogy az alkalmazást meghatározó jogalany felelős a magánélet-védelmi hatásvizsgálat elvégzéséért. Ez a jogalany lehet az adatkezelő vagy az RFID-alkalmazást tervező szolgáltató.

A biometrikus adatok használatával járó sajátos kockázatok miatt a munkacsoport azt ajánlja, hogy az eszköz célját és módszereit meghatározó jogalany az ilyen típusú adatokkal foglalkozó rendszerek tervezési szakaszának szerves részeként hajtsa végre a magánélet-védelmi hatásvizsgálatot. A vizsgálat végrehajtója lehet a gyártó, az integrátor vagy a végső megrendelő.

A magánélet-védelmi hatásvizsgálatnak figyelembe kell vennie a következőket:

- a gyűjtött információk jellege;
- a gyűjtött információk célja;
- a rendszer pontossága, feltéve, hogy fontos határozatokat eredményezhet az egyénre nézve a biometrikus minta egyezése / nem egyezése;
- a jogalap és a jogszerűség; szükséges-e a hozzájárulás;
- az eszközhöz való hozzáférés és az információknak az adatkezelőn belüli belső és külső megosztása, amelyek biztonsági technikákat és eljárásokat tesznek szükségessé a személyes adatok engedély nélküli hozzáférés elleni védelme érdekében;
- a magánéletbe kevésbé beavatkozó intézkedéseket már meghozták; van-e alternatív eljárás a biometrikus eszközön kívül (mint például a személyi igazolvány elkérése);
- a megőrzési időre és az adatok törlésére vonatkozóan meghozott döntések; mit jelent a releváns időtartam; valamennyi adatot ugyanolyan hosszú időre gyűjtenek-e össze; van-e automatikus döntési mechanizmus és megfelelő tartalékeljárás;
- az érintett jogai.

A magánélet-védelmi hatásvizsgálatoknak nemcsak a kockázatok azonosítására kellene összpontosítaniuk, hanem megfelelő adatvédelmi intézkedésekre és arra is figyelmet kellene fordítaniuk, hogy az adatkezelő hogyan talált megfelelő megoldásokat az előző részben azonosított adatvédelmi kockázatok enyhítésére.

Ha a gyártó vagy az integrátor befejezte a magánélet-védelmi hatásvizsgálatot, a biometrikus rendszer beüzemeléséhez további vizsgálat is szükséges lehet, hogy figyelembe vegyék az adatkezelő sajátosságait. Ha egy biometrikus rendszer például beépül a megrendelő informatikai rendszerébe, a megrendelőnek további magánélet-védelmi hatásvizsgálatot kell végeznie, amely a saját informatikai biztonsági intézkedéseit és eljárásait tekinti át.

5.3.2. A biometrikus adatok speciális jellege

A biometrikus adatok különös figyelmet igényelnek, mert az egyedi viselkedési vagy fiziológiai jellemzői felhasználásával egyértelműen azonosítják az egyént.

Ezért a magánélet-védelmi hatásvizsgálatoknak annak az értékelését kellene szolgálniuk, hogy a vizsgált rendszer hogyan kerülheti el vagy csökkentheti jelentős mértékben a következő három kockázatot.

Az első kockázat a személyazonossággal való csalás, különösen az azonosítás és a hitelesítés esetében. A biometrikus eszköznek olyannak kell lennie, hogy ne lehessen csalással megtéveszteni, és biztosítania kell, hogy a megfeleltetés elvégzését megkísérlő személy valóban a rendszerben nyilvántartott személy legyen. Ez a fenyegetés kisebb jelentőségűnek tűnik azon biometrikus adatok esetében, amelyek nem gyűjthetők az érintett tudtán kívül,

mint amilyen az érmintázat[17]. Nagyobb a probléma azonban az ujjlenyomat- vagy arcfelismerő eszközök esetében. Ujjlenyomatok minden tárgyon maradnak a megérintésük után. Az arc is rögzíthető fényképen anélkül, hogy az adott személy tudna arról.

A második kockázat a céltól való eltérés akár maga az adatkezelő, akár egy harmadik fél – köztük a bűnüldöző hatóságok – részéről. Ez a szokásos, a személyes adatokat érintő fenyegetés rendkívül fontossá válik a biometrikus adatok használata esetén. A gyártóknak minden biztonsági intézkedést meg kell hozniuk az adatok bármilyen helytelen használatának elkerülése érdekében, és minden olyan adatot azonnal törölniük kell, amely a továbbiakban nem szükséges a feldolgozás céljából.

Mint bármilyen más adat esetében is, a jogszerűen feldolgozott vagy tárolt biometrikus adatokat vagy a biometrikus adatok forrásait az adatkezelő nem dolgozhatja fel vagy veheti fel semmilyen új vagy eltérő célból, kivéve, ha van új, jogszerű indok az ilyen új adatfeldolgozásra.

A harmadik kockázat az adatok megsértése, amely a biometrikus adatok esetében speciális lépéseket tesz szükségessé attól függően, hogy milyen típusú adatok kerültek veszélybe.
Ha olyan rendszert használnak, amely egy adott biometrikus sablont egy bizonyos kóddá átalakító algoritmus alapján hoz létre biometrikus adatokat, és a biometrikus adatokat vagy az algoritmust ellopják, illetve azok veszélybe kerülnek, akkor ki kell cserélni azokat.
Ha az adatsértés olyan közvetlenül azonosított biometrikus adatok elvesztésével jár, amelyek nagyon közel vannak a biometrikus adatok forrásához, például arcképek vagy ujjlenyomatok, akkor az érintett személyt alaposan tájékoztatni kell, hogy meg tudja védeni magát egy olyan lehetséges jövőbeli incidens esetén, ahol ezeket a sérült biometrikus adatokat használják ellene bizonyítékként.

5.4. Technikai és szervezeti intézkedések

Jellegükből adódóan a biometrikus adatok feldolgozásához speciális technikai és szervezeti intézkedések és óvintézkedések szükségesek az érintetteket az adatok megsértése esetén érő káros hatások megelőzése érdekében – különösen azon kockázatok miatt, hogy a jogszerűtlen eljárás egy adott biometrikus jellemzőnek a referenciasablonból történő, engedély nélküli „rekonstrukciójához” vezet a különböző adatbázisokkal való összekapcsolás céljából annak érdekében, hogy az érintett tudomása nélkül eredeti célokkal össze nem egyeztethető célokra használják fel az adatait, illetve hogy egyes biometrikus adatokat az érintettekre vonatkozó faji vagy egészségügyi információk felfedésére használjanak fel.

5.4.1. Technikai intézkedések

- *A biometrikus sablonok használata*

A biometrikus adatokat lehetőség szerint biometrikus sablonok formájában kell tárolni.

A sablonokat az adott biometrikus rendszerre jellemző módon kell kinyerni, és nem használhatják azokat hasonló rendszerek más adatkezelői. Ennek célja, hogy egy személyt csak azon biometrikus rendszerekben lehessen azonosítani, amelyeknek jogalapjuk van erre a műveletre.

- *Tárolás személyes eszközön / központosított tárolás*

Minden olyan esetben, amikor engedélyezett a biometrikus adatok feldolgozása, jobb elkerülni a személyes biometrikus információk központosított tárolását.

[17] Azt azonban nehéz megjósolni, hogy milyen támadások lesznek lehetségesek az érmintázathoz kapcsolódó technológiát érintően a következő években, ha szélesebb körben használják majd ezt a technológiát.

A munkacsoport – különösen az ellenőrzésre vonatkozóan – ajánlatosnak tartja, hogy a biometrikus rendszerek a kizárólag az adott érintettek birtokában lévő hordozón (például intelligens kártyák vagy hasonló eszközök) titkosított sablon formájában tárolt biometrikus adatok leolvasásán alapuljanak. Az érintettek biometrikus jellemzői közvetlenül az adott kártyára, illetve eszközre vonatkozóan végrehajtott szabványos összehasonlítási eljárásokkal vethetők össze a kártyán, illetve eszközön tárolt sablonnal (sablonokkal), ezáltal általában és lehetőség szerint kerülendő a biometrikus információkat tartalmazó adatbázisok létrehozása. Ha a kártya, illetve az eszköz elveszik, jelenleg alacsony a kockázata annak, hogy az azon szereplő biometrikus információkkal visszaélhessenek. A személyazonosság-lopás kockázatának csökkentése érdekében az ilyen eszközökön csak kevés olyan adatot kellene tárolni, amely az érintetthez kapcsolódik.

Meghatározott célokra és objektív igények esetén azonban megengedhetőnek tekinthetők a biometrikus információkat, illetve sablonokat tartalmazó központosított adatbázisok. Az alkalmazott biometrikus rendszernek és a választott biztonsági intézkedéseknek csökkenteniük kell az említett kockázatokat és gondoskodniuk kell arról, hogy a szóban forgó biometrikus adatok további célokra való újbóli felhasználása lehetetlen legyen, vagy legalább is nyomon követhető. A biometrikus adatok engedély nélküli leolvasásának, másolásának, módosításának vagy eltávolításának megakadályozása érdekében titkosítási technológiákon alapuló mechanizmusokat kell használni.

Ha a biometrikus adatokat olyan eszközön tárolják, amely felett az érintett fizikailag rendelkezik, az adatok engedély nélküli hozzáférés elleni védelmének hatékony biztosítékaként a leolvasó eszközökre vonatkozó speciális titkosítási kulcsot kell alkalmazni. Emellett az ilyen decentralizált rendszerek a kialakításuknál fogva hatékonyabb védelmet biztosítanak a biometrikus adatok számára, mivel az érintett fizikailag ellenőrzése alatt tartja a biometrikus adatait, és nincs egy olyan adott pont, amelyet meg lehetne célozni vagy ki lehetne használni.

A munkacsoport hangsúlyozza azt is, hogy a központosított adatbázis fogalma sokféle technikai megvalósítási módot foglal magába, a leolvasón belüli tárolástól a hálózati adatbázisig.

- *Megújíthatóság és megmásíthatóság*

Mivel a biometrikus adatok forrása nem változtatható meg, a személyazonossági kapcsolat létrehozását célzó biometrikus rendszereket úgy kell megtervezni, hogy a felvételi folyamat és a biometrikus adatok feldolgozása lehetővé tegye, hogy több és egymástól független biometrikus sablon legyen kinyerhető ugyanabból a forrásból, hogy a sablonokat adatsértés vagy technológiai fejlődés esetén ki lehessen cserélni.

A biometrikus rendszereket úgy kell megtervezni, hogy lehetőség legyen a személyazonossági kapcsolat visszavonására, annak megújítása, vagy tartós törlése céljából, például ha visszavonják a hozzájárulást[18].

[18] A TURBINE technológia például olyan módon védi a biometrikus sablont, hogy az ujjlenyomat-információkat titkosítási transzformációval vissza nem fejthető kóddá alakítja, amely lehetővé teszi a bitenkénti összehasonlítás útján való megfeleltetést. Az átalakított biometrikus adatokat a biometrikus mintákra és az eredeti sablonokra visszavezethetetlennek tartják. Ezenkívül a felhasználók bizalmának erősítése érdekében ez a kulcs visszavonható is lesz, azaz új, független kulcs generálható a biometrikus személyazonosságok újbóli létrehozásához. Lásd még:

- *Titkosított forma*

Ami a biztonság kérdését illeti, megfelelő intézkedéseket kell elfogadni a biometrikus rendszer által tárolt és feldolgozott adatok védelme érdekében: a biometrikus információkat mindig titkosított formában kell tárolni. Kulcskezelési keretet kell meghatározni annak biztosítása érdekében, hogy a dekódolási kulcsokhoz csak a szükséges adatok érdekében lehessen hozzáférni.

Tekintettel a biometrikus információkat tartalmazó nyilvános és magánadatbázisok széles körű használatára és a biometriát használó különböző rendszerek egyre növekvő mértékű átjárhatóságára, előnyben kell részesíteni az olyan sajátos technológiák vagy adatformátumok használatát, amelyek lehetetlenné teszik a biometrikus adatbázisok összekapcsolását és az adatok ellenőrzés nélküli közlését.

- *Csalás elleni védelem*

A biometrikus rendszer megbízhatóságának fenntartása és a személyazonossággal elkövetett csalás megakadályozása érdekében a gyártónak olyan rendszereket kell készítenie, amelyek képesek megállapítani, hogy a biometrikus adat valódi-e és továbbra is kapcsolódik-e természetes személyhez. Az arcfelismerést illetően kritikus fontosságú lehet annak biztosítása, hogy az arc valódi legyen, és ne például egy csaló fejére erősített kép.

- *Biometrikus titkosítás és dekódolás*

A biometrikus titkosítás olyan technika, amely biometrikus jellemzőket használ a titkosítási és dekódolási algoritmus részeként. Ebben az esetben általában biometrikus adatok kivonatát használják kulcsként a szolgáltatáshoz szükséges valamely azonosító titkosításához.

Ennek a rendszernek sok előnye van[19]. Nem kerül sor az azonosító vagy a biometrikus adatok tárolására: csak az azonosító biometrikus adatokkal való titkosításának eredményét tárolják. Ezenkívül a személyes adatok visszavonhatók, mivel másik azonosító hozható létre, amelyet szintén biometrikus titkosítással lehet védeni. Ez a rendszer végül pedig biztonságosabb és könnyebben használható az egyén számára: megoldja azt a problémát, amelyet a hosszú és összetett jelszavak észben tartása jelent.

A megoldandó titkosítási probléma azonban nem egyszerű, mivel a titkosítás és a dekódolás nem tűr semmilyen változást a kulcsban, miközben a biometrikus adatok különböző mintát szolgáltatnak, ami változásokat idézhet elő a kinyert kulcsban. A rendszernek ezért képesnek kell lennie arra, hogy némileg eltérő biometrikus adatokból is ugyanazt a kulcsot számítsa ki a hibás elfogadási arány növekedése nélkül.

A munkacsoport egyetért azzal, hogy a biometrikus titkosítási technológia ígéretes kutatási terület és kellően megérett arra, hogy a közpolitika nagyobb figyelmet szenteljen neki, hogy prototípusok fejlesztésére kerüljön sor, és hogy az alkalmazási területeit fontolóra vegyék.

- *Automatikus adattörlési mechanizmusok*

Annak megakadályozása érdekében, hogy a biometrikus információkat több ideig tárolják, mint azt az információk gyűjtésének célja indokolná, vagy hogy később feldolgozzák, megfelelő automatikus adattörlési mechanizmusokat kell létrehozni abban az esetben is, ha a

---

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf.

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

megőrzési időszak jogszerűen meghosszabbítható, biztosítva ezzel a biometrikus rendszer működéséhez szükségtelenné váló személyes adatok időben történő törlését.

Leolvasón való integrált tárolás használata esetén a gyártók a biometrikus sablonok tárolására ún. „felejtő memóriát" alkalmazhatnak, ami garantálja, hogy a leolvasó kikapcsolásakor az adatok törlődnek. Így a leolvasó eladásakor vagy leszerelésekor nem marad biometrikus adatbázis. Leszerelés esetén jelző riasztókat is használhatnak, hogy automatikusan törlődjenek az adatok, ha valaki megpróbálja ellopni a leolvasót.

- *Nagy biometrikus adatbázisok és „gyenge kapcsolatot" használó adatbázisok*

Egyes országok nagy biometriai adatbázisokat használnak, főként két célból: a bűnügyi nyomozások segítése és az azonosító iratok (útlevél, személyi igazolvány, vezetői engedély) kibocsátásának biztosítása érdekében. A bűnügyi nyomozáshoz használt adatbázisok általában a bűnelkövetőkről és a gyanúsítottakról gyűjtik össze az információkat, és egy személy biometrikus adatok alapján való azonosítása érdekében kell kialakítani őket. Ezzel szemben a személyazonossággal való visszaéléssel szembeni küzdelemre használt adatbázisok a teljes populáció biometrikus adatait tartalmazzák, amelyeket csak az adott személy hitelesítésére szabad használni (például ha elveszítette a papírjait vagy megsemmisült az útlevele biztonsági chipje, amely a biometrikus adatokat tárolja).

Ha egy központi adatbázist használnak a személyazonossággal való visszaélés elleni küzdelem céljára, akkor a munkacsoport szerint technikai intézkedéseket kell végrehajtani a céltól való eltérés megakadályozása érdekében. Egyrészről az adatminimalizálás elve megköveteli, hogy csak a személy hitelesítéséhez szükséges adatokat gyűjtsék. A munkacsoport szerint például két ujj lenyomatának összehasonlítása elegendő egy adott személy hitelesítéséhez.

Az adatkezelők másrészről használhatnak „gyenge kapcsolatot" használó adatbázisokat, amelyeknél egy személy személyazonossága nem egyetlen biometrikus adatkészlethez kapcsolódik, hanem biometrikus adatkészletek egy csoportjához. Az adatbázis kialakításának garantálnia kell a személy nagyon nagy valószínűséggel történő hitelesítését (például 99,9 %-kal, amely már elég a csalók elrettentéséhez), és biztosítania kell, hogy az adatbázis ne legyen használható azonosításra (mert egy adott biometrikus adatkészlet sok személynek felel meg).

A munkacsoport támogatja az ilyen rendszerek használatát olyan esetekben, amelyekben nagy biometrikus rendszereket használnak a személyazonossággal való csalás elleni küzdelem céljára.

Példa: hitelesítési rendszerekre vonatkozó technikai intézkedések
A biometrikus adatok forrása egyedi és potenciálisan egész életében kapcsolódik az érintetthez. Ha hitelesítési rendszerek alapjául használják, nem szabad megfeledkezni arról, hogy nem változtatható meg, míg a közönséges hitelesítési technológiák esetén, amelyekhez tipikusan egy igazoló eszköz (például felhasználóazonosító, jelszó) ismerete vagy birtoklása szükséges, mindig lehetséges ennek az igazoló eszköznek a megváltoztatása. Ezért a biometrikus hitelesítést használó rendszerekben speciális biztosítékoknak kell szerepelniük a biometrikus és az egyéb személyazonossági adatok közötti kapcsolat védelme érdekében:

– A sablonok adatai nem tárolhatók központilag, mivel a biometrikus adatok tárolásának biztonsága alapvető fontosságú a biometrikus rendszer általános biztonsága szempontjából. Előnyben kell részesíteni a megosztott tárolást (például intelligens kártyán). Ebben az esetben mind az adatok forrását, mind a sablont az érintett hordozza.
– A biometrikus adatok tárolását és továbbítását megfelelő titkosítási technológiák használatával kell védeni a lehallgatás, engedély nélküli közlés és módosítás ellen.
– Bizonyos típusú biometrikus adatok nem titkosak (például az arc), és nem lehet őket zárolni, blokkolni vagy megváltoztatni az adatok illetéktelen módon történő felhasználása, közlése vagy visszaélés esetén. Ennek következtében a hitelesítést össze kell kapcsolni más zárolható vagy megváltoztatható igazoló eszközökkel.

5.4.2. Szervezeti intézkedések

Az adatvédelem garantálása érdekében szervezeti intézkedéseket kell megtervezni és végrehajtani. Az adatkezelőnek például egyértelmű eljárást kell létrehoznia arra vonatkozóan, hogy ki férhet hozzá a rendszerben szereplő információkhoz, hogy a hozzáférés részleges-e vagy sem, és milyen okokból kerülhet rá sor. Minden cselekményt nyomon kell követni.

A munkacsoport megállapítja, hogy lehetséges a külső szolgáltatóknak való kiszervezés, a vízumkérelmekre vonatkozóan is (a Közösségi Vízumkódex létrehozásáról szóló, 2009. július 13-i 810/2009/EK rendelet 13. és 43. szakasza), ami a felhőben való tárolás (cloud storage) egyre gyakoribb használata miatt egyre népszerűbbé válik.

Ebben az esetben az adatkezelőnek részletes szabályokat kell megállapítania arra vonatkozóan, hogyan ellenőrzi a vállalkozóit, például előre nem bejelentett ellenőrzésekkel, és garanciákat kell kérnie a munkavállalókra, az egyének jogaihoz kapcsolódó eljárásra stb. vonatkozóan.

Kelt Brüsszelben, 2012. április 27-én

a munkacsoport részéről
az elnök
Jacob KOHNSTAMM