05/2022. sz. iránymutatások az arcfelismerő technológia bűnüldözés területén történő alkalmazásáról

2.0 változat

Elfogadás időpontja: 2023. április 26.

A dokumentum eddigi változatai

1.0 változat	2022. május 12.	Az iránymutatások nyilvános konzultáció céljából történő elfogadása
2.0 változat	2023. április 26.	Az iránymutatások nyilvános konzultációt követő elfogadása

Tartalomjegyzék

ÖSSZEFOGLALÓ

Egyre több bűnüldöző hatóság alkalmaz vagy tervez alkalmazni arcfelismerő technológiát (FRT). Az FRT felhasználható egy személy **hitelesítésére** vagy **azonosítására**, és videofelvételeken (pl. CCTV) vagy fényképeken is alkalmazható. Különféle célokra használható, ideértve a rendőrségi figyelőlistákon szereplő személyek felkutatását vagy egy személy közterületen belüli mozgásának nyomon követését is.

Az FRT **biometrikus adatok** kezelésére épül, ezért magában foglalja a személyes adatok különleges kategóriáinak kezelését. Az FRT gyakran használ **mesterséges intelligenciát** (AI) vagy a gépi tanulást (ML). Bár ez széles körű adatkezelést tesz lehetővé, a hátrányos megkülönböztetés és a hamis eredmények kockázatával is jár. Az FRT alkalmazható egyes személyek ellenőrzésére, de hatalmas tömegeken és fontos közlekedési csomópontokon is.

Az FRT **a bűnüldöző hatóságok által használt, érzékeny eszköz.** A bűnüldöző hatóságok szuverén hatáskörökkel rendelkező végrehajtó hatóságok. Az FRT – a személyes adatok védelméhez való jogon túlmenően is – sértheti az alapvető jogokat, és befolyásolni tudja a társadalmi és demokratikus politikai stabilitást.

A személyes adatok bűnüldözéssel összefüggő védelme érdekében teljesíteni kell **a bűnüldözési irányelv (LED) követelményeit**. A LED, különösen 3. cikkének 13. pontja (a „biometrikus adat" fogalma), 4. cikke (A személyes adatok kezelésére vonatkozó elvek), 8. cikke (Az adatkezelés jogszerűsége), 10. cikke (A személyes adatok különleges kategóriáinak kezelése) és 11. cikke (Automatizált döntéshozatal egyedi ügyekben) bizonyos keretet ad az FRT használatára vonatkozóan.

Az FRT alkalmazása számos más alapvető jogot is érinthet. Ezért az **Európai Unió Alapjogi Chartája** („a Charta"), különösen a Charta 8. cikkében foglalt személyes adatok védelméhez való jog, de a Charta 7. cikkében foglalt magánélethez való jog is, alapvető fontosságú a LED értelmezéséhez.

A személyes adatok kezelésének jogalapjául szolgáló **jogalkotási intézkedések** közvetlenül érintik a Charta 7. és 8. cikke által biztosított jogokat. A biometrikus adatok kezelése minden körülmények között önmagában is súlyos beavatkozást jelent függetlenül attól, hogy az milyen eredménnyel (pl. egyezés) jár. Az alapvető jogok és szabadságok gyakorlásának bármilyen korlátozásáról jogszabályban kell rendelkezni, és annak tiszteletben kell tartania e jogok és szabadságok lényegét.

A jogalapnak **kellően egyértelműnek** kell lennie ahhoz, hogy a polgárok megfelelő tájékoztatást kapjanak azokról a feltételekről és körülményekről, amelyek fennállása esetén a hatóságok bármilyen adatgyűjtési vagy titkos megfigyelési intézkedéshez folyamodhatnak. A LED 10. cikkében foglalt általános záradék átültetése a nemzeti jogba önmagában nem lenne elég pontos és előrelátható.

Mielőtt a nemzeti jogalkotó új jogalapot hoz létre a biometrikus adatok arcfelismeréssel történő kezelésének bármely formájához, **konzultálnia** kell az illetékes adatvédelmi felügyeleti hatósággal.

A jogalkotási intézkedéseknek **alkalmasnak** kell lenniük a szóban forgó jogszabályban kitűzött jogszerű célok elérésére. Egy **közérdekű cél** – bármennyire alapvető is – önmagában nem indokolja egy alapvető jog korlátozását. A jogalkotási intézkedéseknek a célkitűzés, például egy konkrét súlyos bűncselekmény elleni küzdelem fényében **meg kell különböztetniük** és meg kell célozniuk az intézkedés hatálya alá tartozó személyeket. Ha az intézkedés ilyen különbségtétel, korlátozás vagy kivétel nélkül általánosságban minden személyre vonatkozik, az fokozza az alapvető jogokba történő beavatkozást. Emellett az is fokozza a beavatkozást, ha az adatkezelés a lakosság jelentős részét érinti.

Az adatokat olyan módon kell kezelni, hogy biztosítva legyen az uniós adatvédelmi szabályok és elvek alkalmazhatósága és hatékonysága. A **szükségesség és az arányosság értékelésénél** minden helyzetben azonosítani kell és figyelembe kell venni az egyéb alapvető jogokra gyakorolt valamennyi lehetséges hatást is. Ha az adatokat szisztematikusan, az érintettek tudta nélkül kezelik, az valószínűleg a **folyamatos megfigyelés általános érzetét** kelti. Ez elrettentő hatást gyakorolhat néhány, vagy valamennyi érintett alapvető jog – így a Charta 1. cikkében foglalt emberi méltóság, a Charta 10. cikkében foglalt gondolat-, lelkiismeret- és vallásszabadság, a Charta 11. cikkében foglalt véleménynyilvánítás szabadsága, valamint a Charta 12. cikkében foglalt gyülekezési és egyesülési szabadság – tekintetében.

A személyes adatok különleges kategóriáinak, például a biometrikus adatoknak a kezelése csak akkor tekinthető „**feltétlenül szükségesnek**" (LED 10. cikk), ha a személyes adatok védelméhez való jogba való beavatkozás és annak korlátozása a feltétlenül szükséges mértékre, azaz az elengedhetetlenre korlátozódik, kizárva minden általános vagy szisztematikus jellegű adatkezelést.

Az a tény, hogy az érintett egy fényképet **kifejezetten nyilvánosságra hozott** (LED 10. cikk), nem jelenti azt, hogy a fényképből speciális technikai eszközökkel kinyerhető, kapcsolódó biometrikus adatok kifejezetten nyilvánosságra hozottnak tekinthetők. Egy szolgáltatás alapértelmezett beállításai, például a sablonok nyilvánosan hozzáférhetővé tétele vagy a választás hiánya, például amikor a sablonok közzétételére anélkül kerül sor, hogy a felhasználó megváltoztathatná ezt a beállítást, semmiképpen nem értelmezhetők kifejezetten nyilvánosságra hozott adatoknak.

A LED 11. cikke létrehozza az **egyedi ügyekben történő automatizált döntéshozatal** keretét. Az FRT használata különleges adatkategóriák használatát vonja maga után, és az alkalmazás módjától és céljától függően, profilalkotáshoz vezethet. Az uniós joggal és a LED 11. cikkének (3) bekezdésével összhangban minden esetben meg kell tiltani a személyes adatok különleges kategóriái alapján történő olyan profilalkotást, amely a természetes személyekre vonatkozóan megkülönböztetést eredményez.

A LED 6. cikke szerint **különbséget kell tenni az érintettek különböző kategóriái között**. Azon érintettek esetében, akiknél nincs olyan bizonyíték, amely arra engedne következtetni, hogy magatartásuk – akár közvetett vagy távoli – kapcsolatban állhat a LED szerinti jogszerű céllal, minden valószínűség szerint nem indokolható a beavatkozás.

Az **adattakarékosság elve** (LED 4. cikk (1) bekezdés e) pont) azt is előírja, hogy az adatkezelés célja szempontjából nem releváns videó anyagokat az üzembe helyezés előtt mindig el kell távolítani vagy anonimizálni kell (pl. elhomályosítással az adatok visszamenőleges helyreállításának lehetősége nélkül).

Bármely FRT-t alkalmazó adatkezelés megkezdése előtt az adatkezelőnek gondosan mérlegelnie kell, hogyan tud (illetve képes-e) megfelelni az **érintettek jogaira** vonatkozó követelményeknek, mivel az FRT gyakran a személyes adatok különleges kategóriáinak kezelésével jár az érintettel való nyilvánvaló interakció nélkül.

Az érintettek jogainak hatékony gyakorlása attól függ, hogy az adatkezelő teljesíti-e **tájékoztatási kötelezettségeit** (LED 13. cikk). Annak értékelésekor, hogy fennáll-e a LED 13. cikk (2) bekezdése szerinti „különleges eset", több tényezőt kell figyelembe venni, beleértve azt is, hogy a személyes adatok gyűjtése az érintett tudta nélkül történik-e, mivel ez az egyetlen módja annak, hogy az érintettek hatékonyan gyakorolhassák jogaikat. Amennyiben a döntéshozatal kizárólag az FRT alapján történik, akkor az érintetteket tájékoztatni kell az automatizált döntéshozatal jellemzőiről.

Ami a **hozzáférés iránti kérelmeket** illeti, ha a biometrikus adatokat alfanumerikus adatok útján is tárolják és kapcsolják össze egy személyazonossággal, az adattakarékosság elvével összhangban ennek lehetővé kell tennie az illetékes hatóság számára, hogy megerősítse az említett alfanumerikus adatok alapján végzett keresésen alapuló hozzáférési kérelmet anélkül, hogy mások biometrikus adatainak további kezelését kezdeményezné (pl. egy adatbázisban FRT-vel történő kereséssel).

Az érintetteket érintő kockázatok különösen súlyosak, ha a pontatlan adatokat rendőrségi adatbázisban tárolják és/vagy más szervezetekkel megosztják. Az adatkezelőnek **helyesbítenie** kell a tárolt adatokat és ennek megfelelően az FRT-rendszereket (lásd még LED (47) preambulumbekezdés).

A **korlátozáshoz való jog** különösen fontossá válik, ha az arcfelismerő technológiát (amely algoritmus(ok)on alapul, ezért soha nem mutat végleges eredményt) olyan helyzetekben használják, amikor nagy mennyiségű adatot gyűjtenek és az azonosítás pontossága és minősége változhat.

Az FRT használatát megelőző **adatvédelmi hatásvizsgálat (DPIA)** kötelező követelmény, vö. LED 27. cikk. Az Európai Adatvédelmi Testület a bizalom és az átláthatóság fokozására szolgáló intézkedésként, az ilyen értékelések eredményeinek, vagy legalább a DPIA főbb megállapításainak és következtetéseinek nyilvánosságra hozatalát ajánlja.

Az FRT üzembe helyezése és használata a legtöbb esetben eredendően magas kockázatot jelent az érintettek jogaira és szabadságaira nézve. Ezért az FRT-t alkalmazni kívánó hatóságnak a rendszer üzembe helyezése előtt **konzultálnia** kell az illetékes felügyeleti hatósággal.

Tekintettel a biometrikus adatok egyedi jellegére, az FRT-t végrehajtó és/vagy használó hatóságnak a LED 29. cikkével összhangban különös figyelmet kell fordítania az **adatkezelés biztonságára**. A bűnüldöző hatóságnak különösen azt kell biztosítania, hogy a rendszer megfeleljen a vonatkozó szabványoknak és alkalmazzon biometrikus-sablon védelmi intézkedéseket. Az adatvédelmi elveket és biztosítékokat a személyes adatok kezelésének megkezdése előtt be kell építeni a technológiába. Ezért még abban az esetben is, ha egy bűnüldöző hatóság külső szolgáltatóktól származó FRT-t kíván alkalmazni és használni, biztosítania kell – pl. a közbeszerzési eljárás révén –, hogy csak olyan FRT-t helyezzenek üzembe, amely a **beépített és alapértelmezett adatvédelem** elvén alapul.

A **naplózás** (vö. LED 25. cikk) fontos biztosíték az adatkezelés jogszerűségének mind belső (pl. az adatkezelő/adatfeldolgozó által végzett önellenőrzés), mind a felügyeleti hatóságok általi külső ellenőrzésére. Az arcfelismerő rendszerekkel összefüggésben ajánlott naplózni a referencia-adatbázis változásait és az azonosítási vagy ellenőrzési kísérleteket, ideértve a felhasználót, az eredményt és a megbízhatósági pontszámot is. A naplózás azonban az **elszámoltathatóság általános elvének** csak egy alapvető eleme (vö. LED 4. cikk (4) bekezdés). Az adatkezelőnek tudnia kell bizonyítani, hogy az adatkezelés megfelel a LED 4. cikkének (1)–(3) bekezdésében foglalt alapvető adatvédelmi elveknek.

Az Európai Adatvédelmi Testület emlékeztet az általa, és az európai adatvédelmi biztossal közösen hozott **felhívásra** néhány adatkezelésitípus **betiltására**: 1) a személy nyilvánosan hozzáférhető térben történő távoli biometrikus azonosítása 2) MI által támogatott arcfelismerő rendszerek, amelyek a személyeket biometrikus adataik alapján etnikai hovatartozásuk, nemük, valamint a politikai vélemény vagy a szexuális irányultság, vagy egyéb tulajdonság szerint kategóriákba sorolják (3) arcfelismerés vagy hasonló technológiák használata természetes személyek érzelmeinek kikövetkeztetésére és 4) személyes adatok bűnüldözéssel összefüggésben történő kezelése, amely a személyes adatok tömeges és megkülönböztetés nélküli gyűjtésével kezelt adatbázisra támaszkodik, pl. online hozzáférhető fényképek és arcképmás „begyűjtése” révén.

A szóban forgó alapvető jogok egyik központi biztosítéka az illetékes adatvédelmi felügyeleti hatóságok általi **hatékony felügyelet**. Ezért a tagállamoknak biztosítaniuk kell, hogy a felügyeleti hatóságok erőforrásai megfelelőek és elegendők legyenek megbízatásuk teljesítéséhez.

A jelen **iránymutatások címzettjei** az uniós és a nemzeti jogalkotók, valamint az FRT-rendszereket bevezető és alkalmazó bűnüldöző hatóságok, és tisztviselőik. A személyekkel általánosságban vagy érintettként foglalkoznak, különös tekintettel az érintettek jogaira.

Az **iránymutatások célja**, hogy tájékoztatást nyújtsanak az FRT bizonyos tulajdonságairól és a bűnüldözéssel összefüggésben alkalmazandó jogi keretről (különös tekintettel a LED-re).

- Ezen túlmenően kínálnak egy, **az adott felhasználási eset érzékenységének első osztályozását segítő eszközt** (I. melléklet).
- Tartalmaznak továbbá **egy gyakorlati útmutatást azon bűnüldöző hatóságok számára, amelyek FRT-rendszert kívánnak beszerezni és működtetni** (II. melléklet).
- Az iránymutatások számos tipikus **felhasználási esetet is bemutatnak és számos releváns szempontot felsorolnak**, különös tekintettel a szükségességi és arányossági tesztre (III. melléklet).

1 BEVEZETÉS

1. Az arcfelismerő technológia (FRT) az egyének arcuk alapján történő automatikus felismerésére használható. Az FRT gyakran mesterséges intelligencián, például gépi tanulási technológiákon alapul. Az FRT-alkalmazásokat egyre gyakrabban tesztelik és használnak különböző területeken, az egyéni felhasználástól kezdve magánszervezeteken át a közigazgatásig. A bűnüldöző hatóságok is előnyöket várnak az FRT használatától. Az FRT megoldást ígér viszonylag új kihívásokra, például olyan nyomozásoknál, ahol nagy mennyiségű lefoglalt bizonyíték áll rendelkezésre, de ismert problémákra is, különös tekintettel a megfigyelési és keresési feladatok ellátásához szükséges személyi állomány hiányára.

2. Az FRT iránti fokozott érdeklődés nagyrészt az FRT hatékonyságának és méretezhetőségének köszönhető. Azonban a technológiában és annak alkalmazásában rejlő, szintén jelentős hátrányokról sem szabad megfeledkezni. Bár egy gombnyomással több ezer személyesadat-állomány elemezhető, az algoritmikus megkülönböztetésnek vagy a téves azonosításnak már enyhe következménye is az lehet, hogy nagy számú személy magatartását és mindennapi életét súlyosan befolyásolja. A személyes adatok, különösen a biometrikus adatok kezelésének már önmagában a mérete az FRT-nek további kulcsfontosságú eleme, mivel a személyes adatok kezelése beavatkozást jelent az Európai Unió Alapjogi Chartájának (a továbbiakban: a Charta) 8. cikke szerinti, személyes adatok védelméhez való alapvető jogba.

3. Az FRT bűnüldöző hatóságok általi alkalmazása jelentős hatással lesz – és bizonyos mértékig már jelentős hatással van – az egyes emberekre és az emberek csoportjaira egyaránt, beleértve a kisebbségeket. Ezek a következmények jelentős hatással lesznek az együttélésünk módjára, valamint társadalmi és demokratikus politikai stabilitásunkra is, amely nagy jelentőséget tulajdonít a pluralizmusnak és a politikai ellenzéknek. A személyes adatok védelméhez való jog gyakran kulcsfontosságú előfeltétele más alapvető jogok biztosításának. Az FRT alkalmazása a személyes adatok védelméhez való jogon túlmenően is jelentősen sértheti az alapvető jogokat.

4. Az Európai Adatvédelmi Testület ezért fontosnak tartja, hogy hozzájáruljon az FRT-nek a bűnüldözés területén az egyes nemzeti jogok által átültetett bűnüldözési irányelv[1] alapján történő folyamatos integrálásához, és ezen iránymutatást adja ki. Az iránymutatás célja, hogy releváns információkat nyújtson az uniós és nemzeti szintű jogalkotók, valamint a bűnüldöző hatóságok és tisztviselőik számára az FRT-rendszerek bevezetése és használata során. Az iránymutatás hatálya az FRT-re korlátozódik. A biometrikus személyes adatok bűnüldöző hatóságok általi kezelésének egyéb formái azonban – különösen távoli adatkezelés esetén – az egyénekre, csoportokra és a társadalomra nézve hasonló vagy további kockázatokat jelenthetnek. Az adott körülményektől függően, az iránymutatás egyes aspektusai ezekben az esetekben is hasznos forrásként szolgálhatnak. Végezetül azok a személyek, akik általában vagy mint érintettek érdeklődnek, szintén fontos információkat találhatnak, különös tekintettel az érintettek jogaira.

5. Az iránymutatás a fő dokumentumból és három mellékletből állnak. A jelen fő dokumentum a technológiát és az alkalmazandó jogi keretet mutatja be. Az I. mellékletben található egy sablon, amely segít meghatározni az alapvető jogokba való beavatkozás súlyosságának egy adott alkalmazási területre történő besorolásához szükséges főbb szempontokat. A II. melléklet az FRT-rendszert beszerezni és működtetni kívánó bűnüldöző hatóságok számára tartalmaz gyakorlati útmutatást. Az FRT alkalmazási területétől függően különböző megfontolások bírhatnak jelentőséggel. A III. mellékletben hipotetikus esetek és a vonatkozó megfontolások leírása található.

2 TECHNOLÓGIA

2.1 Egy biometrikus technológia, két különböző funkció

6. Az arcfelismerés hitelesítés vagy azonosítás céljából alkalmazott valószínűségszámítási technológia, amely képes az egyéneket az arcuk alapján automatikusan felismerni.

7. Az FRT a biometrikus technológia tágabb kategóriájába tartozik. A biometrikus azonosítás magában foglal minden olyan automatizált folyamatot, amely az egyén fizikai, fiziológiai vagy viselkedési jellemzők (ujjlenyomatok, az írisz szerkezete, hang, járás, érmintázat stb.) számszerűsítésén keresztül történő felismerésére szolgál. Ezek a jellemzők „biometrikus adatoknak” minősülnek, mivel lehetővé teszik vagy megerősítik az adott személy egyedi azonosítását.

8. Ilyen például az emberi arc, pontosabban annak arcfelismerő eszközökkel történő technikai kezelése: egy arcról készült felvétel (fénykép vagy videó) – ún. biometrikus minta – alapján leképezhető ezen arc sajátos jellemzőinek digitális megjelenítése (ún. „sablon”).

9. A biometrikus sablon biometrikus mintából leképezett egyedi jellemzők digitális reprezentációja, amely biometrikus adatbázisban tárolható[2]. Ez a sablon elvileg minden személyre nézve egyedi és sajátos, és elvben az idő múlásával tartós[3]. A felismerési szakaszban az eszköz összehasonlítja ezt a sablont más, korábban közvetlenül biometrikus mintákból, például képen, fényképen vagy videón található arcokból létrehozott vagy kiszámított sablonokkal. Az „arcfelismerés” tehát kétlépcsős

[1] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

[2] Iránymutatások az arcfelismerésről, A személyes adatok gépi feldolgozása során az egyének védelméről szóló 108. sz. egyezmény tanácsadó bizottsága, Európa Tanács, 2021 június.

[3] Ez függhet a biometria típusától és az érintett életkorától.

folyamat: az arcképmás gyűjtése és sablonná való átalakítása, ezt követően az arc felismerése a megfelelő sablon egy vagy több másik sablonnal történő összehasonlításával.

10. Bármely más biometrikus folyamathoz hasonlóan, az arcfelismerés is két különböző funkciót tölthet be:

- Egy személy **hitelesítése**, amelynek célja annak igazolása, hogy az adott személy az, akinek mondja magát. Ebben az esetben a rendszer egy előzetesen rögzített (pl. egy intelligens kártyán vagy biometrikus útlevélben tárolt) biometrikus sablont vagy mintát hasonlít össze egyetlen arccal, például egy ellenőrző ponton megjelenő személy arcával, hogy ellenőrizze, egy és ugyanazon személyről van-e szó. Ez a funkció tehát két sablon összehasonlításán alapul. Ezt **igazolásnak** (egy az egyhez megfeleltetés) is nevezik.

- A **személyazonosítás** célja egy személy megtalálása személyek csoportjában, egy adott területen, egy képen vagy egy adatbázisban. Ebben az esetben a rendszernek minden egyes rögzített arcot elemeznie kell, hogy biometrikus sablont hozzon létre, majd ellenőrizze, hogy az egyezik-e a rendszer által ismert személlyel. Ez a funkció tehát egy sablonnak a sablonokat vagy mintákat tartalmazó adatbázissal (kiindulási alap) való összehasonlításán alapul. Ezt egy a többhöz megfeleltetésnek (azonosításnak) is nevezik. Például egy személynév-nyilvántartás (vezetéknév, keresztnév) összekapcsolható egy arccal, ha az összehasonlítás a vezeték- és keresztnevekkel ellátott fényképek adatbázisával történik. A funkció használható egy személy tömegben történő követésére is anélkül, hogy szükségszerűen azonosítanák az adott személyt.

11. Az alkalmazott arcfelismerési technológiák mindkét esetben – az összehasonlítandó és a referencia-adatbázisban található – sablonok közötti becsült egyezésen alapulnak. Ebből a szempontból ezek a technológiák probabilisztikusak: az összehasonlítás alapján nagyobb vagy kisebb valószínűséggel állapítható meg, hogy valóban a hitelesítendő vagy azonosítandó személyről van-e szó; ha ez a valószínűség meghalad egy bizonyos, a felhasználó vagy a rendszer fejlesztője által meghatározott egyezési küszöbértéket a rendszerben, akkor a rendszer feltételezi, hogy van egyezés.

12. Bár a két funkció – a hitelesítés és az azonosítás – elkülönül egymástól, mindkettő azonosított vagy azonosítható természetes személyre vonatkozó biometrikus adatok kezeléséhez kapcsolódik, ezért személyes adatok kezelésének, pontosabban a személyes adatok különleges kategóriái kezelésének minősül.

13. Az arcfelismerés a videókép-feldolgozási technikák szélesebb spektrumának részét képezi. Egyes videókamerák egy meghatározott területen belül filmezhetik az embereket, különösen az arcukat, de önmagukban nem használhatók a személyek automatikus felismerésére. Ugyanez vonatkozik az egyszerű fényképezésre is: a kamera nem arcfelismerő rendszer, mivel az emberekről készült fényképeket a biometrikus adatok leképezése érdekében különleges módon kell feldolgozni.

14. Az úgynevezett „intelligens” kamerák által végzett, önmagában vett arcfelismerés sem feltétlenül minősül arcfelismerő rendszernek. Bár etikai és hatékonysági szempontból ezek is fontos kérdéseket vetnek fel, a rendellenes viselkedés vagy erőszakos események észlelésére, illetve az arc érzelmeinek vagy akár sziluettjének felismerésére szolgáló digitális technikák nem tekinthetők a személyes adatok különleges kategóriáit kezelő biometrikus rendszereknek, feltéve, hogy nem céljuk a személy egyedi azonosítása, és a szóban forgó személyes adat kezelés nem terjed ki a személyes adatok egyéb különleges kategóriáira. Ezek a példák nem állnak teljesen távol az arcfelismeréstől, ezért továbbra is

vonatkoznak rájuk a személyes adatok védelmére vonatkozó szabályok.[4] Továbbá az ilyen típusú felismerő rendszer más, a személy azonosítására irányuló rendszerekkel együtt is használható, és ezáltal arcfelismerő technológiának tekinthető.

15. Ellentétben például a videófelvételi és -feldolgozó rendszerekkel, amelyek fizikai eszközök telepítését igénylik, az arcfelismerés olyan szoftverfunkció, amely meglévő rendszereken (kamerák, képadatbázisok stb.) belül is megvalósítható. Az ilyen funkciók ezért számos rendszerrel összekapcsolhatók és más funkciókkal kombinálhatók. Egy már meglévő infrastruktúrába történő integráció különös figyelmet igényel az abból eredő kockázatok miatt, hogy az arcfelismerési technológia súrlódásmentes és könnyen elrejthető lehet[5].

2.2 A célok és alkalmazások széles skálája

16. Ezen iránymutatások alkalmazási körén és a LED hatályán kívül az arcfelismerés számos különböző célra alkalmazható mind a kereskedelmi felhasználás, mind pedig a közbiztonsággal vagy a bűnüldözéssel kapcsolatos aggályok kezelése területén. Számos különböző kontextusban alkalmazható: egy felhasználó és a szolgáltatás közötti személyes kapcsolatban (hozzáférés az alkalmazáshoz), egy adott helyre történő belépéshez (fizikai szűrés), vagy minden különösebb korlátozás nélkül a nyilvános térben (élő arcfelismerés). Bármilyen típusú érintettre alkalmazható: egy szolgáltatás igénybe vevőjére, munkavállalóra, egyszerű bámészkodóra, keresett személyre, jogi vagy közigazgatási eljárásban érintett személyre stb. Egyes felhasználások már megszokottak és elterjedtek, míg mások jelenleg kísérleti vagy elméleti szakaszban vannak. Bár ez az iránymutatás nem terjed ki az összes ilyen felhasználásra és alkalmazásra, az Európai Adatvédelmi Testület emlékeztet arra, hogy azok csak akkor hajthatók végre, ha megfelelnek az alkalmazandó jogi keretnek, különösen az általános adatvédelmi rendeletnek és a vonatkozó nemzeti jogszabályoknak.[6] Még a LED kontextusában is, az arcfelismerő technológia felhasználásával kezelt adatok a hitelesítési vagy azonosítási funkciókon túlmenően más célokra, például kategorizálásra tovább kezelhetők.

17. Konkrétabban figyelembe vehető a lehetséges felhasználások skálája attól függően, hogy az emberek milyen mértékben rendelkeznek személyes adataik feletti ellenőrzéssel, milyen hatékony eszközökkel rendelkeznek az ilyen ellenőrzés gyakorlásához, milyen joguk van az ilyen technológia bevezetésére és használatára irányuló kezdeményezéshez, milyen következményekkel jár az alkalmazás rájuk nézve (felismerés, illetve fel nem ismerés esetén), illetve milyen mértékű a végrehajtott adatkezelés. A személy személyes eszközén (intelligens kártyán, okostelefonon stb.) tárolt sablonon alapuló arcfelismerés, amely egy erre a célra szolgáló interfészen keresztül hitelesítésre és szigorúan személyes használatra szolgál, nem jelent ugyanolyan kockázatot, mint például a személyazonosítás céljára történő használat egy ellenőrizetlen környezetben, az érintettek aktív közreműködése nélkül, ahol a megfigyelési területre belépő minden egyes arc sablonját összehasonlítják az adatbázisban tárolt, a populáció széles keresztmetszetéből származó sablonokkal. E két szélsőség között a felhasználások rendkívül változatos spektruma található, amelyek a személyes adatok védelmével kapcsolatos kérdéseket vetnek fel.

18. Annak érdekében, hogy pontosabban illusztrálja azt a kontextust, amelyben az arcfelismerő technológiákat jelenleg megvitatják vagy – akár hitelesítés, akár azonosítás céljából – alkalmazzák, az

[4] A LED 10. cikke (vagy az általános adatvédelmi rendelet 9. cikke) azonban alkalmazandó azokra a rendszerekre, amelyeket arra használnak, hogy az egyéneket biometrikus adataik alapján etnikai hovatartozásuk, valamint a politikai vélemény vagy a szexuális irányultság, vagy egyéb tulajdonság szerinti kategóriákba sorolja.
[5] Például a gyakorlatban egyre gyakrabban használt, testen viselt kamerákban.
[6] További iránymutatásért lásd még az Európai Adatvédelmi Testület 2020. január 29-én elfogadott, a személyes adatok videoeszközök révén történő kezeléséről szóló 3/2019. sz. iránymutatását.

Európai Adatvédelmi Testület irányadónak tartja néhány példa említését. Az alábbi példák csupán leíró jellegűek, és nem tekinthetők az adatvédelemmel kapcsolatos uniós jogszabályoknak való megfelelésük előzetes értékelésének.

Példák az arcfelismeréssel történő hitelesítésre

19. A hitelesítés kialakítható úgy, hogy a felhasználók teljes körű ellenőrzést gyakorolhassanak felette, például azért, hogy szolgáltatásokhoz vagy alkalmazásokhoz kizárólag otthoni környezetben férhessenek hozzá. Mint ilyet, az okostelefon-tulajdonosok széles körben használják a készülékük feloldására a jelszavas ellenőrzés helyett.

20. Az arcfelismeréssel történő ellenőrzés azon személy személyazonosságának ellenőrzésére is használható, aki harmadik felek köz- vagy magánszektorbeli szolgáltatásait kívánja igénybe venni. Az ilyen folyamatok tehát lehetőséget nyújtanak arra, hogy egy mobilalkalmazás (okostelefon, táblagép stb.) segítségével digitális identitást hozzanak létre, amely aztán az online közigazgatási szolgáltatásokhoz való hozzáféréshez használható.

21. Az arcfelismeréssel történő hitelesítés célja lehet egy vagy több előre meghatározott helyszínhez, például épületek bejáratához vagy meghatározott átkelőhelyekhez való fizikai hozzáférés ellenőrzése is. Ezt a funkciót például a határátlépés céljából végzett meghatározott adatkezelések során alkalmazzák, ahol egy adott személynek az ellenőrző pont eszközén megjelenő arcát összehasonlítják a személyazonosító okmányában (útlevél vagy tartózkodási engedély) szereplő arccal.

Példák az arcfelismeréssel történő azonosításra

22. Az azonosítás sokféle, még változatosabb módokon alkalmazható. Ezek közé tartoznak különösen – de nem kizárólagosan – az alább felsorolt, az EU-ban jelenleg megfigyelt, kísérleti fázisban lévő vagy tervezett felhasználások:

- ismeretlen személy (áldozat, gyanúsított stb.) személyazonosságának keresése fényképadatbázisban;
- egy személy mozgásának megfigyelése közterületen. Az adott személy arcát összehasonlítják az ellenőrzött területen átutazó vagy korábban megfordult személyek biometrikus sablonjaival, például, ha egy csomagot hátrahagynak vagy bűncselekményt követtek el;
- egy személy útjának és más személyekkel való későbbi interakcióinak rekonstruálása, ugyanazon elemek késleltetett összehasonlítása révén, például a személy kontaktjainak azonosítása érdekében;
- körözött személyek távoli biometrikus azonosítása nyilvános helyeken. A biztonsági kamerák által élőben rögzített arcokat valós időben összevetik a biztonsági erők által vezetett adatbázissal;
- személyek automatikus felismerése egy képen, például a kapcsolataik azonosítására egy arcfelismerést alkalmazó közösségi hálózaton. A képet összehasonlítják a hálózat minden olyan tagjának sablonjaival, akik hozzájárultak ehhez a funkcióhoz, annak érdekében, hogy javaslatot tegyenek ezen kapcsolatok nevesített azonosítására;
- szolgáltatásokhoz való hozzáférés. Egyes pénzkiadó automaták például felismerik az ügyfeleiket azáltal, hogy a kamera által rögzített arcot összehasonlítják a bank által tárolt arcképmások adatbázisával;
- utas utazásának nyomon követése az utazás egy bizonyos szakaszában. Az utazás bizonyos szakaszaiban található kapuknál (poggyászkiadó pontok, beszállókapuk stb.) bejelentkező

személyek valós időben kiszámított sablonját összehasonlítják a rendszerben korábban regisztrált személyek sablonjaival.

23. Mivel az arcfelismerő technológiát a bűnüldözésen kívül számos más területen is alkalmazzák, az adatvédelemmel kapcsolatos uniós vívmányokkal való összhang és az azoknak való megfelelés biztosítása érdekében vitathatatlanul átfogó vitára és szakpolitikai megközelítésre van szükség.

2.3 Megbízhatóság, pontosság és az érintettek kockázatai

24. Mint minden technológia, az arcfelismerés is kihívásokkal járhat az alkalmazás során, különös tekintettel a hitelesítés vagy azonosítás megbízhatóságára és hatékonyságára, valamint általában a „forrás" adatok és az arcfelismerő technológiával történő adatkezelés eredményének minőségére és pontosságára.

25. Az ilyen technológiai kihívások különösen az érintettekre nézve jelentenek kockázatokat, amelyek a bűnüldözés területén a legjelentősebbek vagy legsúlyosabbak, figyelembe véve az érintettekre gyakorolt lehetséges jogi vagy más, őket hasonlóan jelentős mértékben érintő hatásokat. Ebben az összefüggésben érdemes hangsúlyozni azt is, hogy az FRT utólagos használata önmagában nem biztonságosabb, mivel a személyek időben és térben nyomon követhetők. Tehát az utólagos felhasználás is konkrét kockázatokkal jár, amelyeket eseti alapon kell értékelni.[7]

26. Amint arra az EU Alapjogi Ügynöksége 2019-es jelentésében rámutatott, „kihívást jelent az arcfelismerő szoftverek szükséges pontossági szintjének meghatározása: a pontosság értékelésének és megítélésének a feladat, a cél és a felhasználás kontextusától függően számos különböző módja van. Ha a technológiát több millió ember által látogatott helyeken – például vasútállomásokon vagy repülőtereken – alkalmazzák, a hibák viszonylag kis hányada (pl. 0,01%)[8] is azt jelenti, hogy több száz embert helytelenül jelölnek meg. A 3. szakaszban leírtak szerint emellett előfordulhat, hogy bizonyos kategóriákba tartozó személyek esetében másokhoz képest nagyobb a valószínűsége a hibás egyezésnek. A hibaarányok kiszámításának és értelmezésének különböző módjai vannak, ezért körültekintően kell eljárni. Ami a pontosságot és a hibákat illeti, különösen a bűnüldözés szempontjából fontosak azok a kérdések is, hogy egy rendszert mennyire könnyű kijátszani, például hamis arcképmások (úgynevezett „spoofing") segítségével."[9]

27. Ebben az összefüggésben az EDPB emlékeztet arra, hogy az FRT – függetlenül attól, hogy azt hitelesítés vagy azonosítás céljából használják fel – nem biztosít végleges eredményt, hanem annak valószínűségére támaszkodik, hogy két arc vagy arcképmás ugyanannak a személynek felel meg.[10] Ez az eredmény még kevésbé megbízható, ha az arcfelismeréshez használt biometrikus minta rossz minőségű. A bemeneti képek elmosódottsága, a kamera alacsony felbontása, a mozgás és a gyenge fényviszonyok alacsony minőséget eredményezhetnek. Az eredményekre jelentős hatást gyakorló egyéb szempontok a gyakoriság és a spoofing, például amikor a bűnözők megpróbálják elkerülni a kamerák előtti elhaladását, illetve becsapni az FRT-t. Számos tanulmány rávilágított arra is, hogy az algoritmikus feldolgozásból származó ilyen statisztikai eredmények torzításnak is ki vannak téve, ami nevezetesen a forrásadatok minőségéből, valamint a tanítási adatbázisokból vagy más tényezőkből, például az üzembe helyezés helyének megválasztásából adódhat. Rá kell mutatni arra is, hogy az

[7] Lásd a III. mellékletben bemutatott példákat.

[8] Ez a pontossági ráta az idézett jelentésből ered és sokkal jobb értéket tükröz, mint az algoritmusok jelenlegi teljesítménye az FRT alkalmazásokban.

[9] Facial recognition technology: fundamental rights considerations in the context of law enforcement (Arcfelismerő technológia: alapvető jogi megfontolások a bűnüldözés összefüggésében), Az Európai Unió Alapjogi Ügynöksége, 2019. november 21.

[10] Ezt a valószínűséget „megbízhatósági pontszámnak" hívják.

arcfelismerő technológia hatást gyakorol más alapvető jogokra, például a magán- és a családi élet tiszteletben tartására, a véleménynyilvánítás és a tájékozódás szabadságára, a gyülekezési és egyesülési szabadságra stb.

28. Ezért alapvető fontosságú, hogy az arcfelismerő technológia megbízhatóságát és pontosságát a LED 4. cikke szerinti kulcsfontosságú adatvédelmi elveknek való megfelelés értékelése során kritériumként vegyék figyelembe, különös tekintettel a méltányosságra és a pontosságra.

29. Annak hangsúlyozása mellett, hogy a jó minőségű adatok elengedhetetlenek a kiváló minőségű algoritmusokhoz, az Európai Adatvédelmi Testület arra is rámutat, hogy az adatkezelőknek elszámoltathatósági kötelezettségük részeként rendszeresen és módszeresen értékelniük kell az algoritmikus adatkezelést annak érdekében, hogy biztosítsák az ilyen személyesadat-kezelés eredményének pontosságát, méltányosságát és megbízhatóságát. Az FRT-rendszerek értékelése, tanítása és továbbfejlesztése céljából felhasznált személyes adatok csak megfelelő jogalap alapján és a közös adatvédelmi elvekkel összhangban kezelhetők.

3 AZ ALKALMAZANDÓ JOGI KERET

30. Az arcfelismerő technológiák használata elválaszthatatlanul kapcsolódik a személyes adatok kezeléséhez, beleértve az adatok különleges kategóriáit is. Ezen túlmenően, közvetlen vagy közvetett hatást gyakorol számos, az Európai Unió Alapjogi Chartájában rögzített alapvető jogra. Ez különösen vonatkozik a bűnüldözés és a büntető igazságszolgáltatás területére. Ezért az arcfelismerési technológiákat szigorúan az alkalmazandó jogi keretnek megfelelően kell alkalmazni.

31. Az alábbi információkat az FRT-vel kapcsolatos jövőbeni jogalkotási és közigazgatási intézkedések értékeléséhez, valamint a meglévő jogszabályok esetről esetre történő alkalmazása során kell felhasználni. Az egyes követelmények relevanciája az adott körülményektől függően változik. Mivel nem minden jövőbeni körülményt lehet előre látni, csak segítségnek tekinthető és nem értelmezhető kimerítő jellegű felsorolásnak.

3.1 Általános jogi keret – Az Európai Unió Alapjogi Chartája és az emberi jogok európai egyezménye (EJEE)

3.1.1 A Charta alkalmazhatósága

32. Az Európai Unió Alapjogi Chartájának (a továbbiakban: a Charta) címzettjei az uniós intézmények, szervek, hivatalok és ügynökségek, valamint a tagállamok, amikor az uniós jogot hajtják végre.

33. A biometrikus adatok bűnüldözési célú kezelésének a LED 1. cikkének (1) bekezdése szerinti szabályozása elkerülhetetlenül felveti az alapvető jogok tiszteletben tartásának kérdését, különös tekintettel a magánélet és a kapcsolattartás tiszteletben tartására (a Charta 7. cikke) és a személyes adatok védelméhez való jogra (a Charta 8. cikke).

34. A természetes személyekről – beleértve az arcukat is – készült videofelvételek gyűjtése és elemzése személyes adatok kezelésével jár. A kép technikai feldolgozása biometrikus adatokra is kiterjed. A természetes személy arcára vonatkozó adatok idővel és hellyel összefüggésben történő technikai feldolgozása lehetővé teszi az érintett személy magánéletére vonatkozó következtetések levonását. Ezek a következtetések utalhatnak a faji vagy etnikai származásra, az egészségre, a vallásra, a mindennapi élet szokásaira, az állandó vagy ideiglenes tartózkodási helyekre, a napi vagy egyéb

mozgásokra, a végzett tevékenységekre, az adott személyek szociális kapcsolataira és arra a társadalmi környezetre, ahol gyakran megfordulnak. Az FRT alkalmazásával nyilvánosságra kerülő információk széles köre világosan mutatja a személyes adatok védelméhez való jogra (a Charta 8. cikke) és a magánélethez való jogra (a Charta 7. cikke) tett lehetséges hatását.

35. Ilyen körülmények között az sem elképzelhetetlen, hogy a szóban forgó biometrikus (arcra vonatkozó) adatok gyűjtése, elemzése és további kezelése hatással lehet arra, hogy az egyének mennyire érzik úgy, hogy – egy szabad és nyitott társadalom keretei között – szabadon cselekedhetnek. Ez súlyos következményekkel járhat az alapvető jogaik, mint például a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a békés gyülekezéshez és az egyesülési szabadsághoz való joguk (a Charta 1., 10., 11. és 12. cikke) gyakorlására is. Az ilyen adatkezelés egyéb kockázatokkal is jár, mint például az illetékes hatóságok által gyűjtött személyes adatokkal való visszaélés kockázata a személyes adatokhoz való jogellenes hozzáférés és azok felhasználása, a biztonság megsértése stb. miatt. A kockázatok gyakran az adatkezeléstől és annak körülményeitől függenek, mint például a rendőrök vagy más jogosulatlan személyek általi jogellenes hozzáférés és felhasználás kockázata. Egyes kockázatok azonban egész egyszerűen a biometrikus adatok egyedi természetéből fakadnak. A címmel vagy telefonszámmal ellentétben az érintett nem tudja megváltoztatni egyedi jellemzőit, például az arcát vagy az íriszét. A biometrikus adatokhoz való jogosulatlan hozzáférés vagy azok véletlen közzététele ahhoz vezetne, hogy az adatok jelszóként vagy kriptográfiai kulcsként való használata veszélybe kerülne, vagy azokat további, engedély nélküli megfigyelési tevékenységekre lehetne felhasználni az érintett hátrányára.

3.1.2 A Chartában rögzített jogokba való beavatkozás

36. A biometrikus adatok kezelése minden körülmények között önmagában is súlyos beavatkozást jelent függetlenül attól, hogy az milyen eredménnyel (pl. egyezés) jár. A kezelés akkor is beavatkozásnak minősül, ha a biometrikus sablont azonnal törlik, miután a rendőrségi adatbázissal való összevetés nem hozott eredményt.

37. Az érintettek alapvető jogaiba való beavatkozás olyan jogi aktusból fakadhat, amelynek célja vagy hatása az adott alapvető jog korlátozása[11]. Származhat továbbá valamely hatóság azonos célú vagy hatású intézkedéséből, vagy akár a törvény által közigazgatási vagy közhatalmi jogosítványok gyakorlásával megbízott magánjogi szervezet intézkedéséből is.

38. A személyes adatok kezelésének jogalapjául szolgáló jogalkotási intézkedés közvetlenül beavatkozik a Charta 7. és 8. cikke által biztosított jogokba[12].

39. A biometrikus adatok és különösen az FRT használata sok esetben a Charta 1. cikkében biztosított, emberi méltósághoz való jogot is érinti. Az emberi méltóság megköveteli, hogy a személyeket ne mint tárgyakat kezeljék. Az FRT egzisztenciális és rendkívül személyes jellemzőket, az arcvonásokat alakítja át gépileg olvasható formába azzal a céllal, hogy emberi rendszámtáblaként vagy személyi igazolványként használja, ezáltal tárgyiasítva az arcot.

40. Az ilyen adatkezelés más alapvető jogokba, például a Charta 10., 11. és 12. cikkében biztosított jogokba is ütközhet, amennyiben a bűnüldöző hatóságok a releváns videókamerás megfigyeléssel elrettentő hatást kívánnak elérni, vagy az ilyen megfigyelés elrettentő hatást vált ki.

[11] 1992. október 28-i Ter Voort ítélet, C-219/91, ECLI:EU:C:1992:414, 36. és azt követő pontok; 1998. április 28-i Metronome ítélet, C-200/96, ECLI:EU:C:1998:172, 28. pont

[12] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 36. pont; 2013. október 17-i Michael Schwarz ítélet, C-291/12, 23. és azt követő pontok.

41. Emellett az arcfelismerő technológiák bűnüldöző szervek általi használatából eredő lehetséges kockázatokat a Charta 47. és 48. cikke szerinti tisztességes eljáráshoz való jog, illetve az ártatlanság vélelme tekintetében is gondosan meg kell vizsgálni. Az FRT alkalmazásának eredménye, pl. egyezés, nemcsak ahhoz vezethet, hogy egy személyt további intézkedés alá vonnak, hanem döntő bizonyíték is lehet a bírósági eljárásokban. Az FRT hiányosságai, mint például az esetleges torzítások, a hátrányos megkülönböztetés vagy a helytelen azonosítás („hibás egyezés") ezért súlyos következményekkel járhatnak a büntetőeljárásokra nézve is. Ezenkívül a bizonyítékok értékelése során az FRT alkalmazásának eredményét előnyben lehet részesíteni, még akkor is, ha egymásnak ellentmondó bizonyítékok állnak rendelkezésre („automatizálási torzítás").

3.1.3 A beavatkozás indoklása

42. A Charta 52. cikkének (1) bekezdése szerint az alapvető jogok és szabadságok gyakorlása csak jogszabály által, és e jogok lényeges tartalmának tiszteletben tartásával korlátozható. Az arányosság elvére figyelemmel, korlátozásukra csak akkor és annyiban kerülhet sor, ha és amennyiben az elengedhetetlen és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

3.1.3.1 Jogszabályi előírás

43. A Charta 52. cikkének (1) bekezdése előírja a konkrét jogalap követelményét. A jogalapnak kellően egyértelműnek kell lennie ahhoz, hogy a polgárok megfelelő tájékoztatást kapjanak azokról a feltételekről és körülményekről, amelyek fennállása esetén a hatóságok bármilyen adatgyűjtési vagy titkos megfigyelési intézkedéshez folyamodhatnak[13]. A jogszabálynak kellő pontossággal kell meghatároznia a hatóságokra ruházott releváns mérlegelési jogkör terjedelmét és gyakorlásának módját, hogy az egyének számára biztosítsák a védelem minimális szintjét, amelyre egy demokratikus társadalomban a jogállamiság alapján jogosultak[14]. Ezenkívül a jogszerűség megfelelő biztosítékokat követel meg annak biztosítása érdekében, hogy különösen az egyénnek a Charta 8. cikke szerinti jogát tiszteletben tartsák. Ezek az elvek a személyes adatoknak az FRT-rendszerek értékelése, tanítása és továbbfejlesztése céljából történő kezelésére is vonatkoznak.

44. Tekintettel arra, hogy a természetes személyek egyedi azonosítása céljából kezelt biometrikus adatok a LED 10. cikkében felsorolt különleges adatkategóriáknak minősülnek, az FRT különböző alkalmazásai a legtöbb esetben külön jogszabályt igényelnének, amely pontosan leírja az alkalmazást és a felhasználás feltételeit. Ez különösen a bűncselekmények típusaira és adott esetben az ilyen bűncselekmények megfelelő súlyossági küszöbére vonatkozik, többek között annak érdekében, hogy hatékonyan ki lehessen zárni a kisebb súlyú bűncselekményeket.[15]

3.1.3.2 A magánélethez és a személyes adatok védelméhez való alapvető jog lényege (a Charta 7. és 8. cikke)

45. Az alapjogok korlátozásainak az egyes helyzetekben továbbra is biztosítaniuk kell az adott jog lényegének tiszteletben tartását. A lényeg az alkalmazandó alapvető jog lényeges tartalmára vonatkozik[16]. Az emberi méltóságot tiszteletben kell tartani, abban az esetben is, ha valamely jog korlátozásra kerül.[17].

---

[13] EJEB, Shimovolos kontra Oroszország, 68. pont; Vukota-Bojić kontra Svájc.

[14] EJEB, Piechowicz kontra Lengyelország, 212. pont.

[15] Lásd pl. 2022. június 21-i Ligue des droits humains ítélet, C-817/19, ECLI:EU:C:2022:491, 151. és azt követő pontok; 2018. október 2-i Ministerio Fiscal ítélet, C-207/16, ECLI:EU:C:2018:788, 56. pont

[16] 2010. december 22-i DEB Deutsche Energiehandels- und Beratungsgesellschaft GmbH ítélet, C-279/09, ECLI:EU:C:2010:811, 60. pont

[17] Magyarázatok az Alapjogi Chartához, I. cím, Magyarázat az 1. cikkhez, HL C 303., 2007.12.14., 17–35. o.

46. A sérthetetlen lényeg esetleges megsértésére utaló jelek a következők:

- Olyan rendelkezés, amely a személy egyéni magatartásától vagy rendkívüli körülményeitől függetlenül korlátozásokat ír elő[18].
- A bírósághoz fordulás nem lehetséges vagy akadályozott[19].
- A súlyos korlátozást megelőzően az érintett személy körülményeit nem veszik figyelembe[20].
- A Charta 7. és 8. cikkében foglalt jogok vonatkozásában: A kommunikációs metaadatok széles körű gyűjtése mellett az elektronikus kommunikáció tartalmára vonatkozó ismeretek megszerzése sértheti e jogok lényegét[21].
- A Charta 7., 8. és 11. cikkében foglalt jogok vonatkozásában: Olyan jogszabály, amely előírja, hogy az online nyilvános hírközlési szolgáltatásokhoz való hozzáférést biztosító szolgáltatóknak és a tárhely szolgáltatóknak általában és megkülönböztetés nélkül meg kell őrizniük többek között az e szolgáltatásokra vonatkozó személyes adatokat[22].
- A Charta 8. cikkében foglalt jogok vonatkozásában: Az adatvédelem és az adatbiztonság alapelveinek hiánya szintén sértheti a jog lényegét[23].

3.1.3.3 Jogszerű cél

47. A 3.1.3. pontban kifejtettek szerint az alapvető jogok korlátozásának ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét kell szolgálnia.

48. Az Unió elismeri mind az Európai Unióról szóló szerződés 3. cikkében említett célokat, mind pedig a szerződések[24] egyedi rendelkezései által védett egyéb érdekeket, azaz – többek között – a szabadságon, a biztonságon és a jog érvényesülésén alapuló térséget, valamint a bűnmegelőzést és a bűnözés elleni küzdelmet. A világ többi részéhez fűződő kapcsolataiban az Uniónak hozzá kell járulnia a békéhez és a biztonsághoz, valamint az emberi jogok védelméhez.

49. Mások jogainak és szabadságainak védelme a személyek azon jogaira vonatkozik, amelyeket az Európai Unió vagy a tagállamok joga véd. Az értékelést azzal a céllal kell elvégezni, hogy az érintett jogok védelmére vonatkozó követelményeket összeegyeztessék, és megfelelő egyensúlyt teremtsenek közöttük[25].

3.1.3.4 A szükségesség és az arányosság vizsgálata

50. Amennyiben alapvető jogokba történő beavatkozásokról van szó, a nemzeti és az uniós jogalkotó mérlegelési jogköre korlátozottnak bizonyulhat. Ez számos tényezőtől függ, többek között az érintett területtől, a Chartában szereplő, szóban forgó jog jellegétől, a beavatkozás jellegétől és súlyosságától, valamint a beavatkozással elérni kívánt céltól[26]. A jogalkotási intézkedéseknek megfelelőnek kell lenniük a szóban forgó jogszabályban kitűzött jogszerű célok eléréséhez. Az intézkedés továbbá nem

[18]2016. február 15-i J. N. kontra Staatssecretaris van Veiligheid en Justitie ítélet, C-601/15, 52. pont

[19] 2010. október 5-i J. McB. kontra L. E. ítélet, C-400/10, ECLI:EU:C:2010:582, 55. pont

[20] 2006. március 23-i ítélet, C-408/03, ECLI:EU:C:2006:192, 68. pont

[21] 2016. december 21-i Tele2 Sverige ítélet C-203/15, ECLI:EU:C:2016:970, 101. pont hivatkozással a következőkre: 2014. április 8-i Digital Rights Ireland Ltd ítélet, C-293/12 és a 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 39. pont

[22] 2020. október 6-i La Quadrature du Net ítélet, C-512/18, ECLI:EU:C:2020:791, 209. és azt követő pontok

[23]2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 40. pont

[24] Magyarázatok az Alapjogi Chartához, I. cím, Magyarázat az 52. cikkhez, HL C 303., 2007.12.14., 17–35. o.

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.

[26]Vö. 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 47. pont a következő forrásokkal együtt: lásd analógia útján az EJEE 8. cikke tekintetében EJEB H.R., S. és Marper kontra Egyesült Királyság [GC], nos. 30562/04. és 30566/04. sz. EJEB, 2008. V., 102. pont.

lépheti túl az említett célkitűzések eléréséhez megfelelő és szükséges mértéket[27]. Egy általános érdekű célkitűzés – bármennyire alapvető is legyen – önmagában nem indokolja az alapvető jog korlátozását[28].

51. Az EUB állandó ítélkezési gyakorlata szerint a személyes adatok védelmével kapcsolatos eltérések és korlátozások csak a feltétlenül szükséges mértékben alkalmazhatók[29]. Ez egyben azt is jelenti, hogy nem állnak rendelkezésre kevésbé beavatkozó jellegű eszközök a cél eléréséhez. A lehetséges alternatívákat, mint például – az adott céltól függően – a személyzet létszámának növelése, gyakoribb rendfenntartás vagy további közvilágítás, gondosan meg kell határozni és értékelni kell. A jogalkotási intézkedéseknek a célkitűzés, például a súlyos bűncselekmények elleni küzdelem fényében meg kell különböztetniük és meg kell célozniuk az intézkedés hatálya alá tartozó személyeket. Ha az intézkedés ilyen különbségtétel, korlátozás vagy kivétel nélkül általánosságban minden személyre vonatkozik, az fokozza az alapvető jogokba történő beavatkozást[30]. Emellett az is fokozza a beavatkozást, ha az adatkezelés a lakosság jelentős részét érinti[31].

52. A személyes adatoknak a Charta 8. cikkének (1) bekezdésében foglalt kifejezett kötelezettségből eredő védelme különösen fontos a magánélet tiszteletben tartásához való jog (a Charta 7. cikke) szempontjából[32]. A jogszabályoknak egyértelmű és pontos szabályokat kell megállapítaniuk a szóban forgó intézkedés hatályára és alkalmazására vonatkozóan, és biztosítékokat kell előírniuk annak érdekében, hogy azok a személyek, akiknek az adatait kezelték, megfelelő garanciákkal rendelkezzenek ahhoz, hogy hatékonyan megvédhessék személyes adataikat a visszaélés kockázatával, valamint az ilyen adatokhoz való jogosulatlan hozzáféréssel vagy felhasználással szemben[33]. Ilyen biztosítékokra még inkább szükség van akkor, ha a személyes adatok automatikus feldolgozás tárgyát képezik, valamint, ha jelentős az adatokhoz való jogellenes hozzáférés kockázata[34]. Ezen túlmenően az FRT üzembe helyezésének belső vagy külső, például bírósági engedélyezése is biztosítékot jelenthet, és bizonyos súlyos beavatkozások esetén szükségesnek bizonyulhat.[35]

53. [36]A megállapított szabályokat a konkrét helyzethez, például a feldolgozott adatok mennyiségéhez, az adatok jellegéhez, és az adatokhoz való jogellenes hozzáférés kockázatához kell igazítani. Ehhez olyan szabályokra van szükség, amelyek a szóban forgó adatok védelmét és biztonságát egyértelműen és szigorúan biztosítják, azok teljes sértetlensége és bizalmas kezelése érdekében[37].

---

[27] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 46. pont, a következő forrásokkal együtt: 2010. július 8-i Afton Chemical Limited ítélet, C-343/09,ECLI:EU:C:2010:419, 45. pont; 2010. november 9-i Volker und Markus Schecke és Eifert ítélet, C-92/09 és C-93/09, EU:C:2010:662, 74. pont; 2012. október 23-i Nelson és társai és TUI Travels etc. ítélet, C-581-629-283-101/12, EU:C:2013:661, 29. pont

[28]2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 51. pont

[29] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 52. pont, a következő forrásokkal együtt: 2013. november 7-i IPI ítélet, C-473/12, EU:C:2013:715, 39. pont és az idézett ítélkezési gyakorlat.

[30] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 57. pont

[31] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 56. pont

[32] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 53. pont

[33]2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 54. pont, a következő forrásokkal együtt: lásd analógia útján az EJEE 8. cikke tekintetében EJEB Liberty és társai kontra Egyesült Királyság, 2008. július 1., No. 58243/00, 62. és 63. pont; Rotaru kontra Románia, 57-59. pontok, valamint S. és Marper kontra Egyesült Királyság, 99. pont.

[34] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 55. pont, a következő forrásokkal: lásd analógia útján, az EJEE 8. cikke tekintetében, EJEB S. és Marper kontra Egyesült Királyság, 103. pont, és M. K. kontra Franciaország, 2013. április 18., 19522/09. sz. ügy, 35. pont.

[35] EJEB, Szabó és Vissy kontra Magyarország, 73–77. pontok

[36] Lásd még a technikai és szervezési intézkedésekre vonatkozó szigorúbb követelményeket a különleges adatkategóriák feldolgozása esetén, a LED 29. cikkének (1) bekezdése.

[37] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 66. pont

54. Az adatkezelő és az adatfeldolgozó közötti kapcsolat tekintetében nem szabad megengedni, hogy az adatfeldolgozók kizárólag gazdasági megfontolásokat vegyenek figyelembe a személyes adatokra alkalmazandó biztonsági szint meghatározásakor; ez veszélyeztetheti a kellően magas szintű védelmet[38].

55. A jogi aktusnak meg kell határoznia azokat az anyagi és eljárásjogi feltételeket, valamint objektív kritériumokat, amelyek alapján megállapítják az illetékes hatóságok adatokhoz való hozzáférésének és azok későbbi felhasználásának korlátait. Ha az adatkezelésre megelőzés, felderítés vagy büntetőeljárás lefolytatása céljából kerül sor, az érintett bűncselekményeknek kellően súlyosnak kell lenniük ahhoz, hogy igazolják például a Charta 7. és 8. cikkében rögzített alapvető jogokba való beavatkozás mértékét és súlyosságát[39].

56. Az adatokat olyan módon kell kezelni, hogy biztosított legyen az uniós adatvédelmi szabályok és elvek alkalmazhatósága és hatékonysága, különös tekintettel a Charta 8. cikkére, amely kimondja, hogy az adatvédelmi és -biztonsági követelmények tiszteletben tartását független hatóságnak kell ellenőriznie. Ilyen helyzetben releváns lehet az a földrajzi hely, ahol az adatkezelésre sor kerül[40].

57. Ami a személyes adatok kezelésének egyes lépéseit illeti, az adatkategóriák között különbséget kell tenni az elérni kívánt cél szempontjából való lehetséges hasznosságuk vagy az érintett személyek alapján[41]. Az adatkezelés feltételeit, például az adattárolás időtartamát objektív kritériumok alapján kell meghatározni annak biztosítása érdekében, hogy a beavatkozás a feltétlenül szükséges mértékre korlátozódjon[42].

58. A szükségesség és az arányosság értékelésénél minden helyzetben azonosítani kell és figyelembe kell venni az egyéb alapvető jogokra, például a Charta 1. cikkében foglalt emberi méltóságra, a Charta 10. cikkében foglalt gondolat-, lelkiismeret- és vallásszabadságra, a Charta 11. cikkében foglalt véleménynyilvánítás szabadságára, valamint a Charta 12. cikkében foglalt gyülekezési és egyesülési szabadságra gyakorolt valamennyi lehetséges hatást.

59. Továbbá nagy jelentőséget kell tulajdonítani annak, hogy ha az adatokat szisztematikusan, az érintettek tudomása nélkül kezelik, az valószínűleg a folyamatos megfigyelés általános érzetét kelti.[43]. Ez az érintett alapvető jogok némelyike vagy mindegyike tekintetében elrettentő hatással járhat.

60. A bűnüldözésben alkalmazandó arcfelismeréssel kapcsolatos jogalkotási intézkedésekben a szükségesség és arányosság értékelésének megkönnyítése és operacionalizálása érdekében a nemzeti és uniós jogalkotók a rendelkezésre álló, kifejezetten erre a feladatra tervezett gyakorlati eszközöket figyelembe tudják venni. Ilyen különösen az európai adatvédelmi biztos által rendelkezésre bocsátott szükségességi és arányossági eszköztár[44].

[38] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 67. pont
[39] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 60. és 61. pont
[40] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 68. pont
[41] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 63. pont
[42] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 64. pont
[43] 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 37. pont
[44] Európai adatvédelmi biztos: A személyes adatok védelméhez való alapvető jogot korlátozó intézkedések szükségességének értékelése: Eszköztár (2017. április 11.); európai adatvédelmi biztos: Az európai adatvédelmi biztos iránymutatásai a magánélethez és a személyes adatok védelméhez fűződő alapvető jogokat korlátozó intézkedések arányosságának értékeléséről (2019. december 19.)

3.1.3.5 A Charta 52. cikkének (3) bekezdése és 53. cikke (a védelem szintje, az EJEE-vel összefüggésben is)

61. A Charta 52. cikkének (3) bekezdése és 53. cikke szerint a Charta által biztosított azon jogok tartalmát és terjedelmét, amelyek megfelelnek az EJEE-ben biztosított jogoknak, azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek. Míg különösen a Charta 7. cikkének van az EJEE-ben megfelelője, addig a Charta 8. cikke esetében nem ez a helyzet[45]. A Charta 52. cikkének (3) bekezdése nem akadályozza meg azt, hogy az Unió joga kiterjedtebb védelmet nyújtson. Mivel az EJEE nem minősül az uniós jogrendbe formálisan beépült jogforrásnak, az uniós jogszabályokat a Chartában foglalt alapvető jogokra tekintettel kell megalkotni[46].

62. Az EJEE 8. cikke szerint a magán- és családi élet tiszteletben tartásához való jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

63. Az EJEE a korlátozások végrehajtásának módjára vonatkozóan is előírásokat állapít meg. A jogállamiság mellett az egyik alapvető követelmény az előreláthatóság. Az előreláthatóság követelményének értelmében a jogszabály szövegének kellően egyértelműnek kell lennie ahhoz, hogy megfelelő iránymutatást adjon az egyéneknek azokra a körülményekre és feltételekre nézve, amelyek fennállása esetén a hatóságok felhatalmazást kapnak az ilyen korlátozások alkalmazására.[47] Ezt a követelményt az EUB és az uniós adatvédelmi jog is elismeri (vö. 3.2.1.1. pont).

64. Az EJEE 8. cikkében foglalt jogok további részletezését tekintve, a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény rendelkezéseit is [48] teljes mértékben tiszteletben kell tartani. Ugyanakkor figyelembe kell venni, hogy ezek a rendelkezések az irányadó uniós jog fényében csak egy minimumszabályt jelentenek.

3.2 Egyedi jogi keret – a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv

65. A bűnüldözésben érvényesítendő adatvédelemről szóló irányelv (LED) bizonyos keretet biztosít az FRT használatára vonatkozóan. Először is, a LED 3. cikkének 13. pontja meghatározza a „biometrikus adat” fogalmát[49]. További részletekért vö. fentebb 2.1. pont. Másodszor, a 8. cikk (2) bekezdése egyértelművé teszi, hogy az adatkezelés csak akkor jogszerű, ha és amennyiben olyan feladat ellátásához szükséges, amelyet a LED 1. cikke (1) bekezdésében meghatározott célokból végeznek és arról nemzeti jogszabály rendelkezik, amely meghatározza legalább az adatkezelés célkitűzéseit, a kezelendő személyes adatokat és az adatkezelés céljait. A biometrikus adatok tekintetében különös jelentőséggel bíró további rendelkezések a LED 10. és 11. cikkei. A 10. cikket a LED 8. cikkével összefüggésben kell értelmezni[50]. A személyes adatok kezelésére vonatkozó, a LED 4. cikkében

[45] 2016. december 21-i Tele2 Sverige ítélet, C-203/15, ECLI:EU:C:2016:970, 129. pont

[46] 2020. július 16-i ítélet, C-311/18, ECLI:EU:C:2020:559, 99. pont.

[47] Emberi Jogok Európai Bírósága, A COPLAND kontra EGYESÜLT KIRÁLYSÁG ügyben hozott 2007. április 3-i 62617/00 ítélet, 46. pont.

[48] 108. sz. ETS

[49] A LED 3. cikkének 13. pontja: „Biometrikus adat”: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzői vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arcképmás vagy a daktiloszkópiai adat.

[50] A WP258 véleménye a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel (EU 2016/680) kapcsolatos néhány kulcsfontosságú kérdéséről, 7. o.

meghatározott elveket minden esetben be kell tartani, és az FRT-n keresztül történő esetleges biometrikus adatkezelés értékelését ezek alapján kell elvégezni.

3.2.1 Az adatok különleges kategóriáinak bűnüldözési célú kezelése

66. A LED 10. cikke szerint a különleges adatkategóriák, például a biometrikus adatok kezelése csak akkor megengedett, az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciák mellett, ha arra feltétlenül szükség van. Ezen túlmenően az adatkezelés csak akkor megengedett, ha azt az uniós vagy tagállami jog lehetővé teszi, az érintett vagy más természetes személy létfontosságú érdekeinek védelme érdekében vagy ha az ilyen adatkezelés olyan adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott. Ez az általános rendelkezés rámutat a különleges adatkategóriák kezelésének érzékenységére.

3.2.1.1 Uniós vagy tagállami jog lehetővé teszi

67. Ami a szükséges jogalkotási intézkedés típusát illeti, a LED (33) preambulumbekezdése kimondja, hogy „ha ez az irányelv tagállami jogra, jogalapra vagy jogalkotási intézkedésre hivatkozik, ez nem szükségszerűen jelent – az érintett tagállam alkotmányos rendjéből fakadó követelmények sérelme nélkül – valamely parlament által elfogadott jogalkotási eszközt.”[51]

68. A Charta 52. cikkének (1) bekezdése szerint a Charta által elismert jogok és szabadságok gyakorlása „csak a törvény által korlátozható”. Ugyanez jelenik meg az EJEE 8. cikke (2) bekezdésében szereplő „csak a törvényben meghatározott esetekben” kifejezésben is, amely nemcsak az alkalmazandó jogszabályoknak való megfelelést jelenti, hanem – a jogszabály jellegének sérelme nélkül – az adott jogszabály minőségére is utal, előírva, hogy annak összhangban kell állnia a jogállamisággal.

69. A LED (33) preambulumbekezdése kifejti továbbá, hogy „mindazonáltal a tagállami jognak, jogalapnak vagy jogalkotási intézkedésnek világosnak és pontosnak kell lennie, alkalmazása szempontjából pedig kiszámíthatónak kell lennie az érintettek számára, amint azt a Bíróságnak és az Emberi Jogok Európai Bíróságának az ítélkezési gyakorlata megköveteli. A személyes adatok ezen irányelv hatálya alá tartozó kezelését szabályozó tagállami jogban rendelkezni kell legalább a célokról, a kezelendő személyes adatokról, az adatkezelés céljairól, a személyes adatok integritásának és bizalmas jellegének megóvásáról, valamint a személyes adatok megsemmisítésére irányuló eljárásokról.”

70. A nemzeti jogszabály szövegének kellően egyértelműnek kell lennie ahhoz, hogy megfelelő iránymutatást adjon az érintetteknek azokra a körülményekre és feltételekre nézve, amelyek fennállása esetén az adatkezelők felhatalmazást kapnak e korlátozások alkalmazására. Ez magában foglalja az adatkezelés lehetséges előfeltételeit, mint például meghatározott típusú bizonyítékok, vagy bírósági/belső felhatalmazás szükségessége. A vonatkozó jogszabályok technológia semlegesek lehetnek, amennyiben megfelelően szabályozzák a személyes adatok FRT-rendszerek általi kezelésének sajátos kockázatait és jellemzőit. A LED irányelvvel, valamint az Európai Unió Bíróságának (EUB) és az Emberi Jogok Európai Bíróságának (EJEB) ítélkezési gyakorlatával összhangban valóban alapvető fontosságú, hogy az érintettek számára előreláthatók legyenek azok a jogalkotási intézkedések, amelyek célja az arcfelismeréssel kapcsolatos intézkedések jogalapjának biztosítása.

71. Egy jogalkotási intézkedésre nem lehet a biometrikus adatok FRT útján történő, bűnüldözési célú kezelését engedélyező jogszabályként hivatkozni, ha pusztán a LED 10. cikke általános rendelkezésének átültetéséről van szó.

[51]A vizsgált jogalkotási intézkedések típusának összhangban kell lennie az uniós joggal vagy a nemzeti joggal. A korlátozás beavatkozásának mértékétől függően a norma szintjét figyelembe véve nemzeti szinten külön jogszabályi intézkedésre lehet szükség.

72. A biometrikus adatokon kívül a LED 10. cikke egyéb különleges adatkategóriák, például a szexuális irányultság, a politikai vélemény és a vallási meggyőződés kezelését is szabályozza, így az adatkezelés széles körére kiterjed. Ezen túlmenően egy ilyen rendelkezésből hiányoznának azok a konkrét követelmények, amelyek meghatározzák, hogy a bűnüldöző hatóságok milyen körülmények között és milyen feltételek mellett folyamodhatnának az arcfelismerő technológia alkalmazásához. Az egyéb adattípusokra való hivatkozás és a különleges biztosítékoknak a továbbiakban nem részletezett, kifejezett szükségessége miatt a LED 10. cikkét a nemzeti jogba átültető – hasonlóan általános és elvont megfogalmazású – nemzeti rendelkezés nem használható jogalapként a biometrikus adatok arcfelismerés alkalmazásával történő kezeléséhez, mivel nem lenne pontos és előrelátható. A LED 28. cikkének (2) bekezdésével, illetve 46. cikke (1) bekezdésének c) pontjával összhangban, mielőtt a jogalkotó a biometrikus adatok arcfelismerést alkalmazó kezelésének bármely formájára vonatkozó, új jogalapot hozna létre, konzultálnia kell a nemzeti adatvédelmi felügyeleti hatósággal.

3.2.1.2 Feltétlenül szükséges

73. Az adatkezelés csak akkor tekinthető „feltétlenül szükségesnek”, ha a személyes adatok védelméhez való jogba való beavatkozás és annak korlátozása a feltétlenül szükséges mértékre korlátozódik[52]. A „feltétlenül” kifejezés hozzáadása azt jelenti, hogy a jogalkotó szándéka szerint a különleges adatkategóriák feldolgozására csak a szükségesség feltételeinél is szigorúbb feltételek mellett kerülhet sor (lásd fentebb 3.1.3.4. pont). Ezt a követelményt úgy kell értelmezni mint elengedhetetlent. Ez abszolút minimumra korlátozza a bűnüldöző hatóságnak a szükségességi vizsgálat során megengedett mérlegelési jogkörét. Az EUB állandó ítélkezési gyakorlatával összhangban a „feltétlen szükségesség” feltétele szorosan kapcsolódik az objektív kritériumok követelményéhez is azon körülmények és feltételek meghatározása érdekében, amelyek mellett az adatkezelés elvégezhető, kizárva ezáltal minden általános vagy szisztematikus jellegű adatkezelést[53].

3.2.1.3 Kifejezetten nyilvánosságra hozott

74. Annak értékelésekor, hogy az adatkezelés olyan adatokra vonatkozik-e, amelyeket az érintett kifejezetten nyilvánosságra hozott, emlékeztetni kell arra, hogy a fénykép önmagában nem tekinthető szisztematikusan biometrikus adatnak[54]. Ezért az a tény, hogy az érintett a fényképet kifejezetten nyilvánosságra hozta, nem jelenti azt, hogy a fényképből meghatározott technikai eszközökkel lehívható kapcsolódó biometrikus adatokat kifejezetten nyilvánosságra hozottnak kell tekinteni.

75. Mint a személyes adatok esetében általában, ahhoz, hogy a biometrikus adatok az érintett által kifejezetten nyilvánosságra hozottnak tekinthetők legyenek, az érintettnek a biometrikus sablont (és nem egyszerűen az arcképmást) szándékosan, nyílt forráson keresztül szabadon hozzáférhetővé és nyilvánossá kell tennie. Ha a biometrikus adatokat egy harmadik fél hozza nyilvánosságra, nem tekinthető úgy, hogy az adatokat az érintett kifejezetten nyilvánosságra hozta.

76. Ezenkívül az érintett magatartásának értelmezése nem elegendő annak megállapításához, hogy a biometrikus adatokat kifejezetten nyilvánosságra hozták. Az Európai Adatvédelmi Testület úgy véli,

---

[52] A magánélet tiszteletben tartásához való alapvető jogra vonatkozó állandó ítélkezési gyakorlat, lásd 2008. december 16-i Satakunnan Markkinapörssi és Satamedia ítélet, C-73/07, ECLI:EU:C:2008:727, 56. pont; 2010. november 9-i Volker und Markus Schecke és Eifert ítélet, C-92/09 és C-93/09, EU:C:2010:662, 77. pont; 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 52. pont (Digitális jogok); 2015. október 6-i Schrems ítélet, C-362/14, ECLI:EU:C:2015:650, 92. pont.

[53] 2020. október 6-i Privacy International ítélet, C-623/17, ECLI:EU:C:2020:790, 78. pont.

[54] VÖ. általános adatvédelmi rendelet (51) preambulumbekezdés: „A fényképek kezelése nem tekintendő szisztematikusan különleges adatkezelésnek, mivel a fényképekre csak azokban az esetekben vonatkozik a biometrikus adatok fogalommeghatározása, amikor a természetes személyek egyedi azonosítását vagy hitelesítését lehetővé tevő speciális eszközzel kezelik őket.”

hogy közösségi hálózatok vagy online platformok esetében például az a tény, hogy az érintett nem aktivált vagy állított be konkrét adatvédelmi funkciókat, nem elegendő annak megállapításához, hogy ez az érintett kifejezetten nyilvánosságra hozta személyes adatait, illetve hogy ezek az adatok (pl. fényképek) az érintett hozzájárulása nélkül feldolgozhatók biometrikus sablonokká és felhasználhatók azonosítási célokra. Általánosabban fogalmazva, egy szolgáltatás alapértelmezett beállításai, pl. a sablonok nyilvánosan elérhetővé tétele, vagy a választás hiánya, pl. a sablonok nyilvánosságra hozatala anélkül, hogy a felhasználó megváltoztathatná ezt a beállítást, semmiképpen sem értelmezhetők kifejezetten nyilvánosságra hozott adatokként.

3.2.2 Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is

77. A LED 11. cikkének (1) bekezdése értelmében a tagállamok kötelesek általánosan megtiltani a kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló azon döntéseket, amelyek az érintettre nézve hátrányos joghatással járnak vagy őt jelentős mértékben érintik. Ezen általános tilalom alóli kivétel az olyan adatkezelés, ha azt az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintettek jogaira és szabadságaira vonatkozó megfelelő garanciákról is rendelkezik, ideértve legalább az érintett jogát arra, hogy az adatkezelőtől emberi beavatkozást kérjen. A kivétel csak korlátozottan alkalmazható. Ez a kitétel a személyes adatok szokásos (azaz nem különleges) kategóriáira vonatkozik. A LED 11. cikkének (2) bekezdése szerinti mentességre még szigorúbb követelmények, illetve használat vonatkozik. Ez a bekezdés ismételten hangsúlyozza, hogy az első bekezdésben említett döntések nem alapulhatnak különleges adatkategóriákon, azaz különösen a természetes személyek egyedi azonosítását szolgáló biometrikus adatokon. Mentesség csak akkor lehetséges, ha az érintett természetes személy jogainak, szabadságainak és jogos érdekeinek védelmét megfelelő intézkedések biztosítják. Ezt a mentességet a LED 10. cikkével együtt és annak fényében kell értelmezni.

78. Az FRT-rendszertől függően még az FRT eredményeit értékelő emberi beavatkozás sem feltétlenül nyújt önmagában elegendő garanciát az egyének jogainak és különösen a személyes adatok védelméhez való jognak a tiszteletben tartására, figyelembe véve a feldolgozásból eredő esetleges torzítást és hibákat. Továbbá az emberi beavatkozás csak akkor tekinthető biztosítéknak, ha a beavatkozó személy az emberi beavatkozás során kritikusan megkérdőjelezheti az FRT eredményeit. Alapvető fontosságú, hogy a személy képes legyen megérteni az FRT-rendszert és annak korlátait, valamint megfelelően értelmezni az eredményeket. Szükséges továbbá egy olyan munkahely és szervezet létrehozása, amely ellensúlyozza az automatizálási torzítás hatásait, és elkerülik az eredményeknek – például az időhiány, a nehézkes eljárások, a karrierre gyakorolt esetleges káros hatások stb. miatti – kritika nélküli elfogadásának elősegítését.

79. A LED 11. cikkének (3) bekezdése szerint az uniós joggal összhangban tilos az olyan profilalkotás, amely a személyes adatok különleges kategóriái, például a biometrikus adatok alapján természetes személyekkel szembeni megkülönböztetést eredményez. A LED 3. cikkének 4. pontja szerint „profilalkotás” a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz vagy érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják. Annak mérlegelésekor, hogy megfelelő intézkedéseket irányoztak-e elő az érintett jogainak és szabadságainak, valamint az érintett természetes személy jogos érdekeinek védelmére, szem előtt kell tartani, hogy az FRT használata profilalkotáshoz vezethet, attól függően, hogy az FRT-t milyen módon és céllal alkalmazzák. Az uniós joggal és a LED 11. cikkének (3) bekezdésével összhangban,

mindenképpen tilos a személyes adatok különleges kategóriái alapján történő olyan profilalkotás, amely a természetes személyekre vonatkozóan megkülönböztetést eredményez.

3.2.3 Az érintettek kategóriái

80. A LED 6. cikke szerint különbséget kell tenni az érintettek különböző kategóriái között. Ezt a megkülönböztetést adott esetben és amennyire lehetséges, meg kell tenni. A különbségtételnek az adatok feldolgozásának módjában kell megnyilvánulnia. A LED 6. cikkében szereplő példákból következik, hogy a személyes adatok kezelésének főszabály szerint az érintettek kategóriája tekintetében is meg kell felelnie a szükségesség és az arányosság kritériumainak[55]. A példákból az is következik, hogy azon érintettek esetében, akik tekintetében nincs olyan bizonyíték, amely arra engedne következtetni, hogy magatartásuk akár közvetett, akár távoli kapcsolatban állhat a LED szerinti jogszerű céllal, minden valószínűség szerint nem indokolt a beavatkozás[56]. Amennyiben a LED 6. cikke szerinti megkülönböztetés nem alkalmazható vagy lehetséges, a LED 6. cikkében foglalt szabály alóli kivételt szigorúan figyelembe kell venni a beavatkozás szükségességének és arányosságának értékelésekor. Az érintettek különböző kategóriái közötti különbségtétel alapvető követelménynek tűnik a személyes adatok arcfelismerést magában foglaló kezelése során, figyelembe véve a lehetséges hamis pozitív vagy hamis negatív találatokat is, amelyek jelentős hatással lehetnek az érintettekre, és jelentőséggel bírhatnak a nyomozás során.

81. Mint említettük, az uniós jog alkalmazása során tiszteletben kell tartani az Európai Unió Alapjogi Chartájának rendelkezéseit, vö. Charta 52. cikk. A LED által biztosított keretet és kritériumokat ezért a Chartára tekintettel kell értelmezni. Az uniós és tagállami jogszabályok nem lehetnek megengedőbbek ennél az intézkedésnél, és biztosítaniuk kell a Charta teljes körű érvényesülését.

3.2.4 Az érintett jogai

82. Az Európai Adatvédelmi Testület már adott ki iránymutatást az érintettek általános adatvédelmi rendelet szerinti jogainak különböző szempontjairól[57]. A LED hasonló jogokat biztosít az érintettek számára, amivel kapcsolatban a 29. cikk szerinti munkacsoport egy véleményében általános iránymutatást adott, amelyet az Európai Adatvédelmi Testület is jóváhagyott[58]. Meghatározott körülmények között a LED lehetővé teszi e jogok bizonyos mértékű korlátozását. Az ilyen korlátozásokra vonatkozó sajátosságok részletei a „Az érintettek jogainak jogszerű korlátozása” című, 3.2.4.6. pontban találhatók.

83. Bár az érintetteknek a LED III. fejezetében felsorolt valamennyi joga természetesen az arcfelismerő technológia (FRT) segítségével történő személyesadat-kezelésre is vonatkozik, a következő fejezet néhány olyan jogra és szempontra összpontosít, amelyekkel kapcsolatban az iránymutatás különös fontossággal bírhat. Ezenkívül e fejezet és az itt található elemzés feltételezi, hogy a szóban forgó, FRT-vel történő adatkezelés megfelel az előző fejezetben ismertetett jogi követelményeknek.

84. Tekintettel a személyes adatok FRT-n keresztül történő kezelésének jellegére (a személyes adatok különleges kategóriáinak kezelése gyakran az érintettel való látható interakció nélkül) az adatkezelőnek alaposan meg kell fontolnia, hogyan feleljen meg (illetve meg tud-e felelni) a LED

[55] Vö. 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 56–59. pontok
[56] Vö. 2014. április 8-i Kärntner Landesregierung és társai ítélet, C-594/12, 58. pont
[57] Lásd például: 1/2022. sz. EDPB-iránymutatás az érintettek jogairól – Hozzáférési jog és 3/2019. sz. EDPB-iránymutatás a személyes adatok videoeszközökkel történő kezeléséről.
[58] A WP258 véleménye a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel (EU 2016/680) kapcsolatos néhány kulcsfontosságú kérdéséről

követelményeinek, mielőtt bármilyen FRT-n keresztül történő adatfeldolgozást megkezdene. Különösen a következők gondos elemzése szükséges:

- kik az érintettek (gyakran többen, mint az adatkezelés fő célpontját jelentő személy);
- hogyan tájékoztatják az érintetteket az FRT-n keresztül történő adatkezelésről (lásd 3.2.4.1. pont);
- hogyan gyakorolhatják az érintettek a jogaikat (itt a tájékoztatáshoz és a hozzáféréshez való jog, valamint a helyesbítéshez vagy korlátozáshoz való jog érvényesítése különösen nagy kihívást jelenthet abban az esetben, ha az FRT-t az érintettekkel való közvetlen kapcsolatfelvételen alapuló ellenőrzés (egy az egyhez megfeleltetés) kivételével minden esetben alkalmazzák).

3.2.4.1 A jogok és információk tömör, érthető és könnyen hozzáférhető módon történő megismertetése az érintettekkel

85. Az FRT kihívásokat támaszt annak biztosításával kapcsolatban, hogy az érintettek tudomást szerezzenek biometrikus adataik kezeléséről. Különösen nagy kihívást jelent, ha egy bűnüldöző hatóság harmadik féltől származó vagy általa rendelkezésre bocsátott FRT videó anyagot elemez, mivel a bűnüldöző hatóságnak kevés lehetősége van – illetve többnyire nincs is lehetősége – arra, hogy az adatgyűjtés időpontjában (pl. egy helyszíni aláírással) értesítse az érintettet. A LED 4. cikk (1) bekezdésének e) pontjában foglalt minimalizálási elv és a LED 13. cikk (2) bekezdésében foglalt tájékoztatási kötelezettség nem teljesítése kockázatának elkerülése érdekében a biometrikus adatok kezelésének megkezdése előtt mindig el kell távolítani vagy anonimizálni kell (pl. az adatok visszaható hatályú visszaalakításának lehetősége nélküli elhomályosításával) a nyomozás (vagy az adatkezelés célja) szempontjából nem releváns videó anyagokat. Az adatkezelő felelőssége, hogy felmérje, milyen információk lennének fontosak az érintett számára jogai gyakorlása során, illetve biztosítsa a szükséges információk rendelkezésre bocsátását. Az érintettek jogainak hatékony gyakorlása attól függ, hogy az adatkezelő teljesíti-e tájékoztatási kötelezettségeit.

86. A LED-rendelet 13. cikkének (1) bekezdése meghatározza, hogy általában milyen minimális információkat kell az érintett rendelkezésére bocsátani. Ezeket az információkat az adatkezelő honlapján, nyomtatott formában (pl. kérésre elérhető tájékoztató füzetben) vagy más, az érintett számára könnyen hozzáférhető forrásokból lehet biztosítani. Az adatkezelőnek minden esetben biztosítania kell, hogy legalább a következő elemekre vonatkozó információk ténylegesen rendelkezésre álljanak:

- az adatkezelő személye és elérhetőségei, beleértve az adatvédelmi tisztviselő elérhetőségeit is;
- az adatkezelés célja, és hogy az adatkezelés FRT-n keresztül történik;
- panasz benyújtásának joga a felügyeleti hatóságnál és a felügyeleti hatóság elérhetőségei;
- a személyes adatokhoz való hozzáférés, valamint azok helyesbítése, törlése vagy kezelésének korlátozása kérelmezésének joga.

87. Emellett a nemzeti jogban meghatározott olyan különleges esetekben, amelyeknek összhangban kell lenniük a LED[59]13. cikkének (2) bekezdésével, például az FRT-n keresztül történő adatkezelés esetében a következő információkat kell közvetlenül az érintett rendelkezésére bocsátani:

- az adatkezelés jogalapja;

[59] Pl. a német szövetségi adatvédelmi törvény 56. Cikkének (1) bekezdése, amely többek között meghatározza, hogy a fedett műveletek során milyen információkat kell az érintettek rendelkezésére bocsátani

- arra vonatkozó információ, hogy hol gyűjtötték a személyes adatokat az érintett tudomása nélkül;
- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- adott esetben a személyes adatok címzettjeinek kategóriáiról (beleértve a harmadik országbeli címzetteket vagy a nemzetközi szervezeteket is).

88. Míg a LED 13. cikkének (1) bekezdése a nyilvánosság számára elérhetővé tett általános információkról, a LED 13. cikkének (2) bekezdése az adott érintett számára meghatározott esetekben nyújtandó kiegészítő információkról szól, például, ha az adatgyűjtés közvetlenül az érintettől vagy közvetve, az érintett tudomása nélkül történik[60]. A LED 13. cikkének (2) bekezdése nem határozza meg egyértelműen, hogy mi értendő „különleges esetek" alatt. Olyan helyzetekre vonatkozik azonban, amikor az érintettek figyelmét fel kell hívni a kifejezetten rájuk vonatkozó adatkezelésre, és megfelelő tájékoztatást kell nyújtani, hogy az érintettek hatékonyan gyakorolni tudják jogaikat. Az Európai Adatvédelmi Testület úgy véli, egy „különleges eset" fennállásának értékelésekor számos tényezőt kell figyelembe venni, többek között azt is, hogy a személyes adatokat az érintett tudomása nélkül gyűjtik-e, mivel ez lenne az egyetlen módja annak, hogy az érintettek hatékonyan tudják gyakorolni jogaikat. A „különleges esetek" további példája lehet az, amikor a személyes adatokat nemzetközi büntetőjogi együttműködési eljárás keretében tovább kezelik, vagy amikor a személyes adatokat a nemzeti jog szerinti fedett műveletek keretében kezelik. Továbbá a (38) preambulum bekezdésből következik, hogy amennyiben a döntéshozatal kizárólag az FRT alapján történik, akkor az érintetteket tájékoztatni kell az automatizált döntéshozatal jellemzőiről. Ez azt is jelezné, hogy ez egy olyan különleges eset, amikor a LED 13. cikkének (2) bekezdésével összhangban az érintettnek további tájékoztatást kell nyújtani[61].

89. Végezetül meg kell jegyezni, hogy a LED 13. cikkének (3) bekezdése szerint a tagállamok bizonyos célok érdekében olyan jogalkotási intézkedéseket fogadhatnak el, amelyek meghatározott esetekben korlátozzák a tájékoztatási kötelezettséget. Ez annyiban és addig érvényes, amíg az említett intézkedés – kellő tekintettel az érintett természetes személy alapvető jogaira és jogos érdekeire – egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül.

3.2.4.2 A hozzáféréshez való jog

90. Általánosságban az érintettnek joga van ahhoz, hogy pozitív vagy negatív visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és amennyiben a válasz pozitív, jogosult arra, hogy a személyes adatokhoz és a LED 14. cikkében felsorolt további információkhoz hozzáférést kapjon. Ami az FRT-t illeti, ha a biometrikus adatokat alfanumerikus adatok segítségével is tárolják, illetve kapcsolják a személyazonossághoz, akkor az illetékes hatóságnak ezen alfanumerikus adatok szerinti keresés alapján, mások biometrikus adatainak további kezelése (azaz az FRT-vel egy adatbázisban történő keresés) nélkül is helyt kell tudni adni a hozzáférési kérelemnek. Az adattakarékosság elvét tiszteletben kell tartani, és nem szabad több adatot tárolni, mint amennyi az adatkezelés célja szempontjából szükséges.

3.2.4.3 A személyes adatok helyesbítéséhez való jog

91. Mivel az FRT nem biztosít abszolút pontosságot, különösen fontos, hogy az adatkezelők éberen odafigyeljenek a személyes adatok helyesbítésére irányuló megkeresésekre. Előfordulhat, hogy az

[60] A WP258 véleménye a bűnüldözésben érvényesítendő adatvédelemről szóló irányelvvel (EU 2016/680) kapcsolatos néhány kulcsfontosságú kérdéséről, 17–18. o.

[61] Jól jegyezze meg a LED 13. cikk (1) bekezdésében szereplő „az érintett rendelkezésére bocsátani" és a LED 13. cikk (2) bekezdésében szereplő „az érintettet tájékoztatni" kifejezések közötti különbséget. A 13. cikk (2) bekezdése szerint az adatkezelőnek biztosítania kell, hogy a tájékoztatás eljusson az érintetthez, amennyiben a weboldalon közzétett információk nem elegendők.

érintettet az FRT alapján pontatlan kategóriába sorolták, például egy videofelvételen szereplő cselekmény menetének kezdeti feltételezése alapján tévesen a gyanúsítottak kategóriájába sorolták. Az érintetteket érintő kockázatok különösen súlyosak, ha a pontatlan adatokat rendőrségi adatbázisban tárolják és/vagy más szervezetekkel megosztják. Az adatkezelőnek megfelelően helyesbítenie kell a tárolt adatokat és az FRT-rendszereket, lásd a LED (47) preambulumbekezdése.

3.2.4.4 A törléshez való jog

92. Az FRT használata a legtöbb esetben – amennyiben nem ellenőrzésre/ hitelesítésre (egy az egyhez megfeleltetés) használják – az érintettek számos biometrikus adatának kezelésével jár. Ezért fontos, hogy az adatkezelő előzetesen mérlegelje, hol húzódnak a cél és a szükségesség határai, hogy a LED 16. cikke szerinti törlés iránti kérelmet indokolatlan késedelem nélkül el lehessen bírálni (mivel az adatkezelőnek törölnie kell többek között azokat a személyes adatokat, amelyek kezelése meghaladja azt, amit a LED 4., 8. és 10. cikkét követő, alkalmazandó jogszabályok lehetővé tesznek).

3.2.4.5 A korlátozáshoz való jog

93. Amennyiben az érintett vitatja a személyes adatok pontosságát, és azok pontossága vagy pontatlansága nem állapítható meg (vagy ha a személyes adatokat bizonyítás céljából meg kell őrizni), az adatkezelő a LED 16. cikkével összhangban köteles korlátozni az érintett személyes adatait. Ez különösen fontossá válik, ha az arcfelismerő technológiát (amely algoritmus(ok)on alapul, ezért soha nem mutat végleges eredményt) olyan helyzetekben használják, amikor nagy mennyiségű adatot gyűjtenek és az azonosítás pontossága és minősége változhat. A rossz minőségű (pl. egy bűncselekmény helyszínéről származó) videóanyag esetén megnő a hibás egyezések kockázata. Továbbá, ha a figyelőlistán szereplő arcképmásokat nem frissítik rendszeresen, az szintén növeli a hamis pozitív vagy hamis negatív eredmények kockázatát. Ha az adott esetben alapos okkal feltételezhető, hogy a törlés sértheti az érintett jogos érdekeit, a személyes adatok törlése helyett korlátozni kell az adatkezelést, és a korlátozott adatokat csak abból a célból lehet kezelni, amely megakadályozta a törlésüket (lásd LED (47) preambulumbekezdés).

3.2.4.6 Az érintettek jogainak jogszerű korlátozása

94. Ami az adatkezelő tájékoztatási kötelezettségeit és az érintettek hozzáférési jogát illeti, a korlátozások csak akkor megengedettek, ha azokat olyan törvényben rögzítik, amely – kellő tekintettel az érintett természetes személy alapvető jogaira és jogos érdekeire – egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül (lásd LED 13. cikk (3) bekezdés, 13. cikk (4) bekezdés, 15. cikk és 16. cikk (4) bekezdés). Ha az FRT-t bűnüldözési célokra használják, az érintett tájékoztatása vagy az adatokhoz való hozzáférés lehetővé tétele a körülmények miatt valószínűleg hátrányos lenne az elérni kívánt cél szempontjából. Ez vonatkozik például egy bűncselekmény rendőrségi kivizsgálására, valamint a nemzetbiztonság vagy a közbiztonság védelmére.

95. A hozzáférési jog nem jelenti automatikusan az összes információhoz való hozzáférést, például egy büntetőügy esetében, ahol személyes adatok merülnek fel. Életszerű példa a jog korlátozásának megengedettségére a büntetőügyi nyomozás során történő adatkezelés.

3.2.4.7 A jogok gyakorlása a felügyeleti hatóság közreműködésével

96. Azokban az esetekben, amikor a LED III. fejezete szerinti jogok gyakorlása jogszerűen korlátozott, az érintett kérheti az adatvédelmi hatóságot, hogy az adatkezelő által végzett adatkezelés jogszerűségének ellenőrzésével az ő nevében gyakorolja jogait. Az adatkezelő feladata, hogy tájékoztassa az érintettet a jogai ilyen módon történő gyakorlásának lehetőségéről (lásd LED 17. cikk 46. cikk (1) bekezdés g. pont). Az FRT esetében ez azt jelenti, hogy az adatkezelőnek biztosítania kell, hogy megfelelő intézkedések legyenek érvényben az ilyen kérelmek kezelésére, például lehetővé téve

a rögzített anyagok lekérdezését, feltéve, hogy az érintett elegendő információt szolgáltat a személyes adatainak azonosításához.

3.2.5 Egyéb jogi követelmények és biztosítékok

3.2.5.1 Adatvédelmi hatásvizsgálat – 27. cikk

97. Az FRT alkalmazása előtt kötelező az adatvédelmi hatásvizsgálat elvégzése, mivel az adatkezelés – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Tekintettel arra, hogy az FRT használata különleges adatkategóriák szisztematikus automatikus kezelését vonja maga után, feltételezhető, hogy ilyen esetekben az adatkezelőnek főszabály szerint adatvédelmi hatásvizsgálatot kell végeznie. Az adatvédelmi hatásvizsgálatnak ki kell terjednie legalább a tervezett adatkezelési műveletek általános leírására, az adatkezelési műveletek szükségességének és arányosságának a célok szempontjából történő értékelésére, az érintettek jogait és szabadságait érintő kockázatok vizsgálatára, a kockázatok kezelése céljából tervezett intézkedésekre, a személyes adatok védelmére és a rendelkezéseknek való megfelelés igazolására szolgáló garanciákra, biztonsági intézkedésekre és mechanizmusokra. Az EDPB a bizalom és az átláthatóság növelésére szolgáló intézkedésként javasolja az ilyen értékelések eredményeinek, vagy legalább az adatvédelmi hatásvizsgálat főbb megállapításainak és következtetéseinek nyilvánosságra hozatalát[62].

3.2.5.2 Előzetes konzultáció a felügyeleti hatósággal – 28. cikk

98. A LED 28. cikke értelmében az adatkezelőnek vagy az adatfeldolgozónak az adatkezelést megelőzően konzultálnia kell a felügyeleti hatósággal, ha: a) az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés magas kockázattal járna, ha az adatkezelő nem tesz intézkedéseket a kockázat mérséklése céljából; vagy b) az adatkezelés típusa, különösen új technológiák, mechanizmusok vagy eljárások alkalmazása esetén magas kockázatot jelent az érintettek jogaira és szabadságaira nézve. Az ezen iránymutatások 2.3. pontjában leírtak szerint az Európai Adatvédelmi Testület úgy véli, hogy az FRT üzembe helyezése és használata a legtöbb esetben eredendően magas kockázatot jelent az érintettek jogaira és szabadságaira nézve. Ezért az FRT-t üzembe helyező hatóságnak az adatvédelmi hatásvizsgálat elvégzésén kívül a rendszer üzembe helyezése előtt konzultálnia kell az illetékes felügyeleti hatósággal.

3.2.5.3 Az adatkezelés biztonsága – 29. cikk

99. A biometrikus adatok egyedi jellege lehetetlenné teszi, hogy az érintett megváltoztassa azokat, ha – például egy adatsértés következtében – veszélyeztetve lennének. Ezért az FRT-t végrehajtó és/vagy használó hatóságnak a LED 29. cikkével összhangban különös figyelmet kell fordítania az adatkezelés biztonságára. A bűnüldöző hatóságnak különösen azt kell biztosítania, hogy a rendszer megfeleljen a vonatkozó előírásoknak és alkalmazzon biometrikus-sablon védelmi intézkedéseket.[63] Ez a kötelezettség még nagyobb jelentőséggel bír, ha a bűnüldöző hatóság harmadik fél szolgáltatót (adatfeldolgozót) vesz igénybe.

3.2.5.4 Beépített és alapértelmezett adatvédelem – 20. cikk

100. A beépített és alapértelmezett adatvédelem célja a LED 20. cikkével összhangban annak biztosítása, hogy az adatvédelmi elvek és garanciák, például az adattakarékosság és a megőrzési időszak

[62] További információkért lásd WP248 rev.01 Adatvédelmi hatásvizsgálati iránymutatások az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés „valószínűsíthetően magas kockázattal jár-e”.

[63] Lásd például: ISO/IEC 24745 Információbiztonság, kiberbiztonság és adatvédelem – Biometrikusinformáció-védelem.

korlátozása, megfelelő technikai és szervezési intézkedések segítségével – például álnevesítéssel – már a személyes adatok feldolgozásának megkezdése előtt beépüljenek a technológiába, és a személyes adatok teljes életciklusa során alkalmazásra kerüljenek. Tekintettel a természetes személyek jogaira és szabadságaira jelentett eredendően magas kockázatra az intézkedések alkalmazása nem függhet kizárólag gazdasági megfontolásoktól[64], hanem inkább a legkorszerűbb adatvédelmi technológiák alkalmazására kell törekedni. Ugyanígy, ha egy bűnüldöző hatóság külső szolgáltatóktól származó FRT-t kíván alkalmazni és használni, biztosítania kell – pl. a közbeszerzési eljárás révén –, hogy csak a beépített és alapértelmezett adatvédelem elvein alapuló FRT-t helyezzenek üzembe.[65]Ez egyben azt is jelenti, hogy az FRT működésének átláthatóságát nem korlátozzák üzleti titkok vagy szellemi tulajdonjogokra vonatkozó igények.

3.2.5.5 Naplózás – 25. cikk

101. A LED különböző módszereket ír elő arra, hogy az adatkezelő vagy az adatfeldolgozó bizonyítsa az adatkezelés jogszerűségét, valamint biztosítsa az adatok sértetlenségét és biztonságát. E tekintetben a rendszernaplók nagyon hasznos eszközt és fontos biztosítékot jelentenek az adatkezelés jogszerűségének mind belső (azaz önellenőrzés), mind külső felügyeleti hatóságok, például az adatvédelmi hatóságok általi ellenőrzéséhez. A LED 25. cikke értelmében legalább a következő adatkezelési műveleteket automatizált adatkezelési rendszerben kell naplózni: gyűjtés, megváltoztatás, betekintés, közlés – ideértve a továbbítást is –, összekapcsolás, illetve törlés. Ezen túlmenően a betekintésre és a közlésre vonatkozó naplók lehetővé kell, hogy tegyék e műveletek indokoltságának, dátumának és időpontjának, valamint – lehetőség szerint – a személyes adatba betekintő vagy azt közlő személyek személyazonosságának, illetve az ilyen személyes adatok címzettjei személyazonosságának a megállapítását. Továbbá az arcfelismerő rendszerekkel összefüggésben ajánlott a következő további adatkezelési műveletek naplózása (részben az LED 25. cikkén túlmenően):

- A referencia adatbázis módosítása (hozzáadás, törlés vagy frissítés). A naplónak meg kell őriznie a vonatkozó (hozzáadott, törölt vagy frissített) kép másolatát, ha más módon nem lehetséges az adatkezelési műveletek jogszerűségének vagy eredményének ellenőrzése.

- Azonosítási vagy ellenőrzési kísérletek, beleértve az eredményt és a megbízhatósági pontszámot. Szigorú minimalizálási elvet kell alkalmazni annak érdekében, hogy a referenciakép tárolása helyett csak a referencia-adatbázisból származó kép azonosítója maradjon meg a naplókban. A bemeneti biometrikus adatok naplózását kerülni kell, kivéve, ha erre szükség van (pl. csak találatok esetén).

- Az azonosítási vagy ellenőrzési kísérletet kérő felhasználó azonosítója.

- A rendszerek naplóiban tárolt személyes adatokra szigorú célhoz kötöttség (pl. ellenőrzés) vonatkozik, és azok nem használhatók fel más célokra (pl. arra, hogy továbbra is el lehessen végezni a referencia adatbázisokból törölt képet tartalmazó felismerést/ellenőrzést). Biztonsági intézkedéseket kell alkalmazni a naplók sértetlenségének biztosítása érdekében, és a naplókkal való visszaélés felderítésére szolgáló automatikus ellenőrző rendszerek kifejezetten ajánlottak. A referencia adatbázis naplói esetében az arcképek tárolása esetén a biztonsági intézkedéseknek a referencia adatbázisra vonatkozókkal egyenértékűnek kell lenniük. Emellett a naplókra vonatkozó

[64] Lásd LED (53) preambulumbekezdés

[65] További információkért lásd: az Európai Adatvédelmi Testület iránymutatása a beépített és alapértelmezett adatvédelemről, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

adatmegőrzési időszak betartásának biztosítása érdekében automatikus folyamatokat kell bevezetni.

3.2.5.6 Elszámoltathatóság – 4. cikk (4) bekezdés

102. Az adatkezelőnek tudnia kell bizonyítani, hogy az adatkezelés megfelel a LED 4. cikk (1)–(3) bekezdésében foglalt elveknek, vö. LED 4. cikk (4) bekezdés. E tekintetben kulcsfontosságú a rendszer (beleértve a frissítéseket, a korszerűsítéseket és az algoritmus tanítását is), a technikai és szervezési intézkedések (beleértve a rendszer teljesítményének nyomon követését és az esetleges emberi beavatkozást is), és a személyes adatok kezelésének szisztematikus és naprakész dokumentációja. Az adatkezelés jogszerűsége bizonyításának különösen fontos eleme a LED 25. cikke szerinti naplózás (vö. 3.2.5.5. pont). Az elszámoltathatóság elve nemcsak a rendszerre és az adatkezelésre vonatkozik, hanem az olyan eljárási garanciák dokumentálására is, mint a szükségesség és arányosság értékelése, az adatvédelmi hatásvizsgálatok, valamint a belső konzultációk (pl. a projekt vezetés általi jóváhagyása vagy a megbízhatósági pontszámok értékére vonatkozó belső döntések) és a külső konzultációk (pl. az adatvédelmi hatósággal). A II. melléklet e tekintetben számos elemet tartalmaz.

3.2.5.7 Hatékony felügyelet – 47. cikk

103. Az illetékes adatvédelmi hatóságok általi hatékony felügyelet az egyik legfontosabb garancia az FRT használata által érintett egyének alapvető jogainak és szabadságainak védelmére. Ugyanakkor az egyes adatvédelmi hatóságok számára a szükséges emberi, technikai és pénzügyi erőforrások, helyiségek és infrastruktúra biztosítása előfeltétele annak, hogy a hatóságok feladataikat hatékonyan el tudják látni és hatáskörüket gyakorolni tudják[66]. Még a rendelkezésre álló személyzet létszámánál is fontosabbak a szakértők készségei, akiknek – a bűnügyi nyomozásoktól és a rendőrségi együttműködéstől kezdve a nagy adathalmazok elemzésén át a mesterséges intelligenciáig – a problémák igen széles köréhez kell érteniük. Ezért a tagállamoknak biztosítaniuk kell, hogy a felügyeleti hatóságok erőforrásai megfelelőek és elegendők legyenek ahhoz, hogy eleget tudjanak tenni az érintettek jogainak védelmére vonatkozó megbízatásuknak és szorosan figyelemmel tudják kísérni az ezzel kapcsolatos fejleményeket.[67]

4 KÖVETKEZTETÉS

104. Az arcfelismerő technológiák használata elválaszthatatlanul kapcsolódik a személyes adatok kezeléséhez, beleértve az adatok különleges kategóriáit is. Az arc és a biometrikus adatok általában tartósan és visszavonhatatlanul kapcsolódnak az adott személy személyazonosságához. Ezért az arcfelismerés alkalmazása közvetlen vagy közvetett hatást gyakorol számos, az Európai Unió Alapjogi Chartájában rögzített alapvető jogra és szabadságra, amelyek túlmutathatnak a magánélethez és az adatvédelemhez való jogon. Ilyen például az emberi méltóság, a mozgás szabadsága, a gyülekezés szabadsága stb. Ez különösen vonatkozik a bűnüldözés és a büntető igazságszolgáltatás területére.

105. Az Európai Adatvédelmi Testület tisztában van azzal, hogy a bűnüldöző hatóságoknak a lehető legjobb eszközökre van szükségük a terrorcselekmények vagy más súlyos bűncselekmények elkövetőinek gyors azonosításához. Ezeket az eszközöket azonban az alkalmazandó jogi keret szigorú tiszteletben tartásával kell alkalmazni, és csak olyan esetekben, amelyek megfelelnek a Charta 52. cikkének (1)

[66] Lásd „Első jelentés a bűnüldözésben érvényesítendő adatvédelemről szóló (EU) 2016/680 irányelv alkalmazásáról és működéséről” című bizottsági közlemény, COM(2022) 364 final, 3.4.1. pont

[67] Lásd: Az Európai Adatvédelmi Testület hozzájárulása a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv (LED) Európai Bizottság általi értékeléséhez, 62. cikk (14) bekezdés, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

bekezdésében meghatározott szükségesség és arányosság követelményeinek. Ezen túlmenően, bár a modern technológiák a megoldás részét képezhetik, semmiképpen sem számítanak csodafegyvernek.

106. Vannak olyan esetek, amikor az arcfelismerő technológiák használata elfogadhatatlanul magas kockázatot jelent az egyének és a társadalom számára („vörös vonalak”). Ezen okok miatt az Európai Adatvédelmi Testület és az európai adatvédelmi biztos ezek általános betiltására szólított fel[68].

107. Ilyen különösen az egyének nyilvános térben történő távoli biometrikus azonosítása, amely az egyének magánéletébe való beavatkozás nagy kockázatát hordozza magában, és nincs helye egy demokratikus társadalomban, mivel természeténél fogva tömeges megfigyeléssel jár. Hasonlóképpen, az Európai Adatvédelmi Testület szerint azok az MI által támogatott arcfelismerő rendszerek sem egyeztethetők össze a Chartával, amelyek az egyéneket biometrikus adataik alapján etnikai hovatartozásuk, nemük, valamint a politikai vélemény vagy a szexuális irányultság, vagy egyéb tulajdonság szerinti kategóriákba sorolják. Az EDPB továbbá meg van győződve arról, hogy az arcfelismerésnek vagy hasonló technológiáknak a természetes személyek érzelmeinek kikövetkeztetésére történő használata rendkívül nemkívánatos, és – néhány kellően indokolt kivételtől eltekintve – be kellene tiltani. Emellett az Európai Adatvédelmi Testület úgy véli, hogy a személyes adatok olyan bűnüldözéssel kapcsolatos kezelése, amely a személyes adatok tömeges és megkülönböztetés nélküli gyűjtésével – például online elérhető fényképek és arcképmások, különösen a közösségi hálózatokon keresztül rendelkezésre bocsátott fényképek és arcképmások „gyűjtésével” (scraping) – feltöltött adatbázison alapulna, mint ilyen, nem felelne meg az uniós jog által előírt szigorú szükségességi követelménynek.

5 MELLÉKLETEK

I. melléklet: Támogatási minta

II. melléklet: Gyakorlati útmutató a bűnüldöző hatóságoknál megvalósítandó FRT-projektek irányításához

III. melléklet: Gyakorlati példák

[68]Lásd Az Európai Adatvédelmi Testületnek és az európai adatvédelmi biztosnak a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatra vonatkozó közös véleménye https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

I. MELLÉKLET – A FORGATÓKÖNYVEK LEÍRÁSÁRA SZOLGÁLÓ SABLON

(A forgatókönyvben tárgyalt szempontokhoz kapcsolódó szövegdobozokkal)

Az adatkezelés leírása:

- Az adatkezelés leírása, Kontextus (bűncselekménnyel fennálló kapcsolat), Cél

Az információ forrása:

- Az érintettek típusai: ☐ minden állampolgár ☐ elítéltek ☐ gyanúsítottak ☐ gyermekek ☐ egyéb kiszolgáltatott érintettek

- A kép forrása: ☐ nyilvános terek ☐ internet ☐ magánszervezet ☐ egyéb magánszemélyek ☐ egyéb .....

- Bűncselekménnyel fennálló kapcsolat: ☐ Közvetlen időbeli ☐ Nem közvetlen időbeli ☐ Közvetlen földrajzi ☐ Nem közvetlen földrajzi ☐ Nem szükséges

- Az információgyűjtés módja: ☐ távoli ☐ egy fülkében vagy ellenőrzött környezetben
- Egyéb alapvető jogokat érintő kontextus:
  ☐ Nem
  Igen, nevezetesen ☐ a gyülekezési szabadság
  ☐ A véleménynyilvánítás szabadsága
  ☐ más alapvető jog:.....
- Az érintettre vonatkozó további lehetséges információforrások:
  ☐ Személyazonosító okmány☐ nyilvános telefonhasználat ☐ gépjármű rendszámtábla
  ☐ egyéb .....

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☐ általános célú adatbázisok ☐ a bűnözés területéhez kapcsolódó speciális adatbázisok
- Annak leírása, hogy ezeket a referencia-adatbázisokat hogyan töltötték fel (és a jogalap)
- Az adatbázis rendeltetésének megváltoztatása (pl. magántulajdon biztonsága volt az elsődleges cél): ☐ IGEN

  ☐NEM

Algoritmus:

- Az adatkezelés típusa:☐ egy az egyhez megfeleltetés útján történő ellenőrzés (hitelesítés)☐ azonosítás (egy a többhöz megfeleltetés)
- A pontossággal kapcsolatos megfontolások
- Technikai biztosítékok

Eredmény

- Hatás ☐ Közvetlen (pl. az érintettet letartóztathatják, kihallgathatják, diszkriminatív magatartás)

  ☐ Nem közvetlen (statisztikai modellekhez használják, nincs komoly jogi lépés az érintettel szemben)

- Automatizált döntés: ☐ IGEN ☐ NEM
- A tárolás időtartama

Jogi elemzés:

- A szükségesség és az arányosság elemzése – cél/a bűncselekmény súlyossága/a bűncselekményben nem érintett, de az adatkezelés által érintett személyek száma
- Az érintett előzetes tájékoztatásának típusa: ☐ Az adott területre való belépéskor

  ☐ A bűnüldöző hatóság honlapján található általános információ

  ☐ A konkrét adatkezeléssel kapcsolatban a bűnüldöző hatóság honlapján található információ

  ☐ Egyéb .....
- Alkalmazandó jogi keret:

  ☐ A LED nagyrészben a nemzeti jogba átültetve

  ☐ A biometrikus adatok bűnüldöző hatóságok általi felhasználására vonatkozó általános nemzeti jogszabály

  ☐ Az ilyen adatkezeléssel (arcfelismerés) kapcsolatban az adott illetékes hatóságra vonatkozó, konkrét nemzeti jogszabály

  ☐ Az ilyen adatkezelésre (automatizált döntés) vonatkozó konkrét nemzeti jogszabály

Következtetés:

Általános megfontolások arra vonatkozóan, hogy a leírt adatkezelés valószínűleg összeegyeztethető-e az uniós joggal (és néhány utalás a jogi előfeltételekre)

II. MELLÉKLET – GYAKORLATI ÚTMUTATÓ A BŰNÜLDÖZŐ HATÓSÁGOKNÁL MEGVALÓSÍTANDÓ FRT-PROJEKTEK IRÁNYÍTÁSÁHOZ

Ez a melléklet további gyakorlati iránymutatást nyújt az arcfelismerő technológiával (FRT) kapcsolatos projekt elindítását tervező bűnüldöző hatóságok számára. Több információt nyújt a projekt megvalósítása során figyelembe veendő szervezési és technikai intézkedésekről, és nem tekintendő az egyes lépések/intézkedések kimerítő felsorolásának. Az útmutatót az Európai Adatvédelmi Testületnek a személyes adatok videóeszközökkel történő kezeléséről szóló 3/2019. sz. iránymutatásával[69], valamint a mesterséges intelligencia használatával kapcsolatos, bármely uniós/EGT rendelettel és az Európai Adatvédelmi Testület iránymutatásaival együtt kell értelmezni.

Az ebben a mellékletben szereplő iránymutatások azon a feltételezésen alapulnak, hogy a bűnüldöző hatóságok (kész termékként) be fogják szerezni az FRT-t. Ha a bűnüldöző hatóság az FRT fejlesztését (további tanítását) tervezi, további követelmények vonatkoznak a fejlesztés során szükséges tanítási, validálási és tesztelési adatkészletek, valamint a fejlesztési környezethez kapcsolódó szerepek/intézkedések kiválasztására. Hasonlóképpen előfordulhat, hogy egy készen kapható terméket a tervezett felhasználáshoz kell igazítani, amely esetben meg kell felelni a tesztelési, validálási és tanítási adathalmazok kiválasztására vonatkozó, fent említett követelményeknek.

Az ugyanazon bűnüldözési hatósághoz tartozás önmagában nem biztosít teljes körű hozzáférést a biometrikus adatokhoz. A személyes adatok más kategóriáihoz hasonlóan a meghatározott jogalap alapján bizonyos bűnüldözési célból gyűjtött biometrikus adatok megfelelő jogalap nélkül nem használhatók fel más bűnüldözési célra (a bűnüldözésben érvényesítendő adatvédelemről szóló (EU) 2016/680 irányelv (LED) 4. cikkének (2) bekezdése). Az FRT-eszköz fejlesztése/tanítása is más célnak minősül, ezért meg kell vizsgálni, hogy a biometrikus adatoknak a teljesítmény mérése/a technológia tanítása céljából történő kezelése, az érintettekre hátrányos alacsony teljesítmény elkerülése érdekében, az adatfeldolgozás eredeti céljára figyelemmel szükséges és arányos-e.

1. SZEREPKÖR ÉS FELELŐSSÉG

Ha a bűnüldöző hatóság FRT-ket alkalmaz a LED hatálya alá tartozó feladatai (bűncselekmények megelőzése, nyomozása, felderítése vagy büntetőeljárás lefolytatása stb., a LED 3. cikke alapján) ellátására, akkor az FRT vonatkozásában adatkezelőnek tekinthető. A bűnüldöző hatóságok azonban több olyan egységből/osztályból állnak, amelyek – akár az FRT-alkalmazás folyamatának meghatározásával, akár annak gyakorlati alkalmazásával – részt vesznek az ilyen adatkezelésben. E technológia sajátosságai miatt előfordulhat, hogy különböző egységek járulnak hozzá a teljesítmény méréséhez vagy a rendszer tanításához.

Az FRT-vel kapcsolatos projektekben számos érdekelt fél[70] részvétele lehet szükséges a bűnüldöző hatóságokon belül:

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[70] A következő szerepek az FRT projektekben részt vevő különböző érdekelt feleket és felelősségeiket mutatják be. Bár az e mellékletben található szerepek leírására használt nyelvezet nem meghatározó, minden egyes bűnüldöző hatóságnak a szervezetétől függően hasonló szerepeket kell definiálnia és kiosztania. Előfordulhat,

- Felső vezetés – a kockázatok és a lehetséges előnyök mérlegelését követően jóváhagyja a projektet.
- Adatvédelmi tisztviselő és/vagy a bűnüldöző hatóság jogi osztálya – segítséget nyújt egy adott FRT projekt végrehajtása jogszerűségének értékelésében; közreműködik az adatvédelmi hatásvizsgálat elvégzésében; biztosítja az érintettek jogainak tiszteletben tartását és gyakorlását.
- Folyamatgazda – az illetékes bűnüldöző hatóságon belül a projekt fejlesztéséért felelős speciális egységként jár el, dönt az FRT-projekt részleteiről, beleértve a rendszer teljesítményére vonatkozó követelményeket is; dönt a megfelelő méltányossági mutatóról; meghatározza a bizalmi pontszámot[71]; meghatározza a torzítás elfogadható küszöbértékeit; (az adatvédelmi tisztviselővel és az IT MI és/vagy adattudományi osztállyal – lásd lentebb – folytatott konzultáció útján) meghatározza az FRT-projekt által az egyének jogaira és szabadságaira jelentett potenciális kockázatokat és bemutatja azokat a felső vezetésnek. A folyamatgazda az FRT-projekt részleteiről való döntés előtt a referencia-adatbázis kezelőjével is konzultál annak érdekében, hogy megértse mind a referencia-adatbázis felhasználási célját, mind annak technikai részleteit. A beszerzett FRT újratanítása esetén a folyamatgazda felel a tanítási adatállomány kiválasztásáért is. A projekt kidolgozásával és a részletekről való döntéssel megbízott egységként a folyamatgazda felelős az adatvédelmi hatásvizsgálat elvégzéséért.
- IT MI és/vagy Adattudományi Osztály – közreműködik az adatvédelmi hatásvizsgálat elvégzésében; magyarázattal szolgál a rendszer teljesítményének, méltányosságának[72] és potenciális torzításának mérésére rendelkezésre álló mutatókra vonatkozóan; az összegyűjtött adatokhoz való jogosulatlan hozzáférés, kibertámadások stb. megelőzésére szolgáló technológia és a technikai garanciák végrehajtása. A beszerzett FRT újratanítása esetén az IT MI vagy adattudományi osztály a folyamatgazda által rendelkezésre bocsátott tanítási adatkészlet alapján tanítja a rendszert. Ez az osztály felel a folyamatgazdák által közösen azonosított kockázatok (pl. MI-specifikus kockázatok, mint például a modell következtetési támadások) csökkentésére irányuló intézkedések meghozataláért is.
- Végfelhasználók (például a helyszínen vagy igazságügyi laboratóriumokban dolgozó rendőrök) – elvégzik az adatbázissal való összehasonlítást; kritikusan felülvizsgálják az eredményeket a korábbi bizonyítékok figyelembevételével, valamint a folyamatgazdáknak visszajelzést adnak a hibás egyezésekről és a lehetséges megkülönböztetésre utaló jelekről.
- Referenciaadatbázis-kezelő – az illetékes bűnüldöző hatóságon belül a referencia-adatbázis összeállításáért és kezeléséért, valamint az arcképmásoknak a meghatározott megőrzési időszak utáni törléséért felelős külön egység. A referencia-adatbázis az az adatbázis, amellyel a képeket összehasonlítják. Ezt az adatbázist létrehozhatják kifejezetten a tervezett FRT-projekt számára, vagy használhatnak már korábban is létező, kompatibilis célokra létrehozott adatbázist. A referenciaadatbázis-kezelő feladata, hogy (idő vagy egyéb kritériumok alapján) meghatározza az adatmegőrzési követelményeket, valamint, hogy mikor és milyen körülmények között tárolhatók az arcképmások.

hogy egy adott egység egynél több szerepet tölt be, például egyszerre folyamatgazda és referenciaadatbázis-kezelő, vagy folyamatgazda és IT MI és/vagy adattudományi osztály (amennyiben a folyamatgazda egysége rendelkezik az összes szükséges technikai ismerettel).

[71] A megbízhatósági pontszám az előrejelzés (egyezés) megbízhatósági szintje valószínűség formájában. Például két sablon összehasonlításával 90%-os a valószínűsége annak, hogy azok ugyanahhoz a személyhez tartoznak. A megbízhatósági pontszám eltér az FRT teljesítményét jelzőtől, de hatással van a teljesítményre. Minél magasabb a megbízhatósági küszöbérték, annál kevesebb hibás egyezés és több hibás „nincs egyezés" eredmény jelenik meg az FRT találatai között.

[72] A méltányosságot úgy lehet meghatározni, mint a tisztességtelen, jogellenes megkülönböztetés, például a nemi vagy faji sztereotípiák hiányát.

Mivel az FRT üzembe helyezése és használata a legtöbb esetben eredendően magas kockázatot jelent az érintettek jogaira és szabadságaira nézve, az adatvédelmi felügyeleti hatóságot is be kell vonni a LED 28. cikkében előírt előzetes konzultációba.

2. ELLENŐRZÉS/AZ FRT-RENDSZER BESZERZÉSE ELŐTT

A bűnüldöző hatóság folyamatgazdájának először is világosan meg kell ismernie az FRT használatát célzó folyamat(ok)at (a felhasználási eset(ek)et), és biztosítania kell, hogy a tervezett felhasználási esetnek legyen jogalapja. Ennek alapján a következőket kell megtenniük:

- A felhasználási eset hivatalos ismertetése. Ismertetni kell a megoldandó problémát és az arra az FRT által nyújtott megoldást, valamint a folyamatot (feladatot), amelyben alkalmazni fogják. E tekintetben a bűnüldöző hatóságoknak legalább a következőket kell dokumentálniuk[73]:
  - A folyamat során rögzített személyes adatok kategóriái
  - Azok a célkitűzések és konkrét célok, amelyekre az FRT-t alkalmazni fogják, beleértve a találatot követően az érintettre gyakorolt lehetséges következményeket is.
  - Az arcképmások gyűjtésének időpontja és módja (beleértve az adatgyűjtés kontextusára vonatkozó információkat, pl. a repülőtéri kapuban, biztonsági kamerák által készített felvételek egy olyan raktár előtt, ahol bűncselekmény elkövetésére került sor, stb., valamint az érintettek azon kategóriái, akiknek biometrikus adatait kezelik).
  - Az adatbázis, amellyel a képeket összehasonlítják (referencia-adatbázis), valamint a létrehozásának módjára, méretére és a benne található biometrikus adatok minőségére vonatkozó információk.
  - A bűnüldöző hatóság azon szereplői, akik jogosultak lesznek az FRT-rendszer használatára és a bűnüldözési környezetben történő felhasználására (profiljaikat és hozzáférési jogaikat a folyamatgazdának kell meghatároznia).
  - A bevitt adatok tervezett megőrzési időszaka vagy az az időpont, amely meghatározza ennek az időszaknak a végét (például a nemzeti eljárási joggal összhangban a büntetőeljárás lezárása vagy megszüntetése, amelyhez az adatokat eredetileg gyűjtötték), valamint minden későbbi intézkedés (ezen adatok törlése, anonimizálása és statisztikai vagy kutatási célokra történő felhasználása stb.).
  - Naplózás végrehajtása, valamint a nyilvántartott naplók és a nyilvántartások hozzáférhetősége.
  - A teljesítménymutatók (pl. pontosság, precizitás, visszahívás, F1-pontszám) és azok minimálisan elfogadható küszöbértékei.[74]
  - Becslés arról, hogy az egyes időszakokban/esetekben az FRT alkalmazása hány személyre lesz hatással.

[73] Az I. melléklet felsorolja azokat az elemeket, amelyek segítik az adatkezelőt egy FRT-felhasználási eset ismertetésében.

[74] Az FRT-rendszer teljesítményének értékelésére különböző mutatók állnak rendelkezésre. Mindegyik mutató más-más képet ad a rendszer eredményeiről, és az adott FRT felhasználási esettől függ, hogy sikerül-e megfelelő képet adni arról, hogy az FRT-rendszer jól teljesít-e vagy sem. Ha a hangsúly egy arc nagy százalékban helyes összevetésén van, akkor olyan mutatók használhatók, mint a pontosság és a visszahívás. Ezek a mutatók azonban nem mérik, hogy az FRT mennyire jól kezeli a negatív példákat (a rendszer hány hibás találatot adott). A folyamatgazdának az IT MI és az adattudományi osztály támogatásával képesnek kell lennie arra, hogy meghatározza a teljesítménykövetelményeket, és azokat az FRT felhasználási esetnek legmegfelelőbb mutatóban fejezze ki.

- A szükségesség és az arányosság értékelése[75]. A technológia meglétének ténye nem lehet az FRT alkalmazásának mozgatórugója. A folyamatgazdának először meg kell vizsgálnia, hogy létezik-e megfelelő jogalap a tervezett adatkezeléshez. Ehhez konzultálnia kell az adatvédelmi tisztviselővel és a jogi szolgálattal. Az FRT üzembe helyezésének mozgatórugója az kell, hogy legyen, hogy az szükséges és arányos megoldás a bűnüldöző hatóság egy konkrétan meghatározott problémájára. Ezt a cél/a bűncselekmény súlyossága/az FRT-rendszer által érintett, de a bűncselekményben nem érintett személyek száma alapján kell értékelni. A jogszerűség értékeléséhez legalább a következőket kell figyelembe venni: LED[76], az általános adatvédelmi rendelet (GDPR)[77] [78] a mesterséges intelligenciára (MI) vonatkozó bármely meglévő jogi keret[79] és az adatvédelmi felügyeleti hatóságok által biztosított valamennyi kísérő iránymutatás (az Európai Adatvédelmi Testület 3/2019. sz. iránymutatása a személyes adatok videó eszközök révén történő kezeléséről[80]). Ezeket az uniós jogi aktusokat mindig alá kell támasztani az alkalmazandó nemzeti követelményekkel, különösen a büntető eljárásjog területén. Az arányosság értékelése során meg kell határozni az esetlegesen érintetteknek (a magánélet és a személyes adatok védelmén túlmenő) alapvető jogait. Ismertetni kell továbbá, illetve figyelembe kell venni az adott használati esetben az FRT-rendszerre vonatkozó korlátokat (vagy a korlátok hiányát). Például, ha a rendszer folyamatosan vagy ideiglenesen működik, és ha a használata egy adott földrajzi területre korlátozódik.
- Adatvédelmi hatásvizsgálat (Data Protection Impact Assessment, DPIA)[81]. Azért kell adatvédelmi hatásvizsgálatot végezni, mert az FRT bűnüldözési területen történő alkalmazása nagy kockázatot jelent az egyének jogaira és szabadságaira nézve[82]. Az adatvédelmi hatásvizsgálatnak különösen a

[75] A rendszer testreszabása és használata tekintetében fontolóra lehet venni a szükségesség biztosítását célzó további lépéseket, így a szükségesség és az arányosság értékelése során a használati eset leírása is kis mértékben módosulhat.

[76] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/680 irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

[77] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.

[78] Azokban az esetekben, amikor az FRT használatának kutatására irányuló tudományos projekt keretében személyes adatok kezelésére kerülne sor, de az ilyen adatkezelés nem tartozna a LED 4. cikke (3) bekezdésének hatálya alá, általában a GDPR alkalmazandó (a LED 9. cikkének (2) bekezdése). Olyan kísérleti projektek esetében, amelyeket bűnüldözési műveletek követnének, a LED továbbra is alkalmazandó lenne.

[79] Létezik például egy JAVASLAT A MESTERSÉGES INTELLIGENCIÁRA VONATKOZÓ HARMONIZÁLT SZABÁLYOK MEGÁLLAPÍTÁSÁRÓL (A MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ JOGI AKTUS) ÉS EGYES UNIÓS JOGALKOTÁSI AKTUSOK MÓDOSÍTÁSÁRÓL SZÓLÓ EURÓPAI PARLAMENTI ÉS TANÁCSI RENDELETRE, a rendeletet azonban még nem fogadták el.

[80]https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Az adatvédelmi hatásvizsgálatokra vonatkozó további iránymutatás a következő címen érhető el: Iránymutatás adatvédelmi hatásvizsgálat elvégzéséhez, valamint annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár-e” (WP248 rec.01), amely a következő címen érhető el: https://ec.europa.eu/newsroom/article29/items/611236 és Az európai adatvédelmi biztos elszámoltathatósága az alap eszközkészlettel kapcsolatban, II. rész, amely a következő címen érhető el: https://edps.europa.eu/node/4582_en

[82]A felhasználási esettől függően az FRT az alábbi kritériumok alapján a magas kockázatú adatkezelés hatálya alá tartozhat (Iránymutatás az adatvédelmi hatásvizsgálatról, WP 248 rev.01): Szisztematikus nyomon követés, nagy mennyiségű adat kezelése, adatkészletek összevetése vagy kombinálása, innovatív felhasználás, vagy új technológiai vagy szervezési megoldások alkalmazása.

következőket kell tartalmaznia: a tervezett adatkezelési műveletek általános leírása[83], az érintettek jogait és szabadságait érintő kockázatok vizsgálata[84], a kockázatok kezelése céljából tervezett intézkedések, a személyes adatok védelmére és a rendelkezésekkel való összhang igazolására szolgáló garanciák, biztonsági intézkedések és mechanizmusok. Az adatvédelmi hatásvizsgálat egy állandó folyamat, ezért az adatkezelés minden új elemét hozzá kell adni, és a kockázatértékelést a projekt minden szakaszában aktualizálni kell.

- A felső vezetés általi jóváhagyás az érintettek jogait és szabadságait érintő (a felhasználási esetből és a technológiából eredő) kockázatok és a vonatkozó kockázatkezelési tervek ismertetésével.

3. A KÖZBESZERZÉS SORÁN ÉS AZ FRT ÜZEMBE HELYEZÉSE ELŐTT

- Az FRT (algoritmus) kiválasztási kritériumainak meghatározása. A folyamatgazdának az IT MI és/vagy az Adattudományi osztály segítségével kell eldöntenie, hogy milyen kritériumok alapján választja ki az algoritmust. A gyakorlatban ide tartoznak a méltányosságra és a teljesítményre vonatkozó, a felhasználási eset leírásában meghatározott mutatók. Ezeknek a kritériumoknak az olyan adatokra vonatkozó információkat is tartalmazniuk kell, amelyekkel az algoritmust tanították. A torzítás csökkentése érdekében a tanítási, tesztelési és validálási adathalmaznak kellően sok mintát kell tartalmaznia az FRT által várhatóan érintett személyek valamennyi jellemzőjéből (például életkor, nem és faj). Az FRT-szolgáltatónak információkat és mutatókat kell szolgáltatnia az FRT tanítási, tesztelési és validálási adatkészleteiről, és ismertetnie kell a potenciális jogellenes megkülönböztetés és torzítás mérése és mérséklése érdekében hozott intézkedéseket. A folyamatgazdának lehetőség szerint (a szolgáltató által rendelkezésre bocsátandó információk alapján) ellenőriznie kell, hogy volt-e jogalap ahhoz, hogy a szolgáltató ezt az adatkészletet az algoritmusok tanítása céljából felhasználja. A folyamatgazdának arról is gondoskodnia kell, hogy az FRT-szolgáltató a biometrikus adatokra vonatkozó biztonsági szabványokat (például az ISO/IEC 24745 szabvány) alkalmazzon, amely a biometrikus adatok tárolás és továbbítás során történő védelmére, a bizalmas jellegre, az integritásra és a megújíthatóságra/visszavonhatóságra, valamint a biometrikus adatok biztonságos és a magánélet védelmét tiszteletben tartó kezelésére és feldolgozására vonatkozó iránymutatásokat tartalmaz.

- Az algoritmus újratanítása (ha szükséges). A folyamatgazdának biztosítania kell, hogy az FRT-rendszernek a használatát megelőzően a nagyobb pontosság érdekében történő finomhangolása a beszerzett szolgáltatások részét képezze. Amennyiben a beszerzett FRT-rendszer további tanítása szükséges a pontossági mutatók teljesítéséhez, a folyamatgazdának az újbóli tanításról szóló döntés meghozatalán túl az IT MI és/vagy az Adattudományi osztály segítségével döntenie kell a megfelelő, reprezentatív adathalmazról, és ellenőriznie kell az adatok felhasználásának jogszerűségét.
- Megfelelő garanciák meghatározása a biztonsággal, a torzítással és az alacsony teljesítménnyel kapcsolatos kockázatok kezelésére. Ez magában foglalja egy eljárás létrehozását az FRT használatának nyomon követésére (naplózás és visszajelzés az eredmények pontossága és méltányossága érdekében). Ezen túlmenően biztosítani kell a gépi tanulásra és FRT-rendszerekre

[83] Az adatkezelés leírása, valamint a szükségesség és arányosság értékelése a fenti lépésekben leírtak szerint a kockázatértékelés mellett az adatvédelmi hatásvizsgálat részét is képezik. Szükség esetén a személyes adatok áramlásának részletesebb leírását az adatvédelmi hatásvizsgálat tartalmazza.

[84] Az érintettekre vonatkozó kockázatok elemzésének ki kell terjednie az összehasonlítandó arcképmások helyével kapcsolatos kockázatokra (helyi/távoli), az adatfeldolgozókkal/alfeldolgozókkal kapcsolatos kockázatokra, valamint adott esetben a gépi tanulásra vonatkozó kockázatokra (pl. adatmérgezés, ellentmondásos példák).

jellemző kockázatok (pl. adatmérgezés, ellentmondásos példák, modell inverzió, white-box következtetés) azonosítását, mérését és mérséklését. A folyamatgazdának továbbá megfelelő garanciákat kell meghatároznia az újratanítási adatkészletben szereplő biometrikus adatokra vonatkozó adatmegőrzési követelmények tiszteletben tartásának biztosítására.

- Az FRT-rendszer dokumentálása. Ennek magában kell foglalnia az FRT-rendszer általános ismertetését, az FRT-rendszer elemeinek és a rendszer létrehozására irányuló folyamatnak a részletes leírását, az FRT-rendszer nyomon követésére, működésére és ellenőrzésére vonatkozó részletes információkat, valamint a kockázatok és a kockázatcsökkentő intézkedések részletes leírását. Az ebben a dokumentációban szereplő elemek tartalmazzák az FRT-rendszer leírásának a korábbi fázisokból (lásd fentebb) származó főbb elemeit, azonban ezek kiegészülnek a teljesítmény nyomon követésével és a rendszer módosításaival kapcsolatos információkkal, beleértve a verziófrissítéseket és/vagy újratanításokat is.
- A technológiát és a felhasználási eseteket bemutató felhasználói kézikönyvek létrehozása. Ezeknek világosan ismertetniük kell minden olyan forgatókönyvet és előfeltételt, amely alapján az FRT-t alkalmazni fogják.
- A végfelhasználók betanítása a technológia használatára. Az ilyen képzéseknek ki kell térniük a technológia képességeire és korlátaira, hogy a felhasználók megértsék, milyen körülmények között szükséges azt alkalmazni, illetve mely esetekben lehet pontatlan. Az ilyen képzések segítenek az algoritmus eredménye ellenőrzésének elmulasztásával/kritizálásával kapcsolatos kockázatok mérséklésében is.
- A LED 28. cikke (1) bekezdésének b) pontja értelmében az adatvédelmi felügyeleti hatósággal történő konzultáció. Az érintettek tájékoztatása az adatkezelésről és a jogaikról, a LED 13. cikke alapján. A tájékoztatást olyan nyelven kell nyújtani, hogy az érintettek képesek legyenek megérteni az adatkezelést, és annak ki kell terjednie a technológia alapvető elemeire, beleértve a pontossági arányokat, a képzési adatkészleteket és a diszkrimináció és az algoritmus alacsony pontosságának elkerülése érdekében hozott intézkedéseket is.

4. AJÁNLÁSOK AZ FRT ÜZEMBE HELYEZÉSÉT KÖVETŐ IDŐSZAKRA

- Az emberi beavatkozás és az eredmények felügyeletének biztosítása. Soha nem szabad semmilyen, az egyént érintő intézkedést kizárólag az FRT eredménye alapján meghozni (ez a LED 11. cikkének megsértését jelentené – az érintettre nézve joghatással vagy más hasonló hatással járó automatizált döntéshozatal egyedi ügyekben). Gondoskodni kell arról, hogy a bűnüldöző hatóság egy tisztviselője felülvizsgálja az FRT eredményeit. Azt is biztosítani kell, hogy a bűnüldöző hatóságok felhasználói az egymásnak ellentmondó információk vizsgálata és a technológia eredményeinek kritikus megkérdőjelezése révén elkerüljék az automatizálási torzítást. Ezért fontos ezt a végfelhasználókban tudatosítani és a végfelhasználókat folyamatos képzésben részesíteni, valamint a felső vezetésnek gondoskodnia kell arról, hogy a hatékony felügyelet elvégzéséhez megfelelő emberi erőforrások álljanak rendelkezésre. Ez azt jelenti, hogy minden egyes ügynöknek elegendő időt kell biztosítani ahhoz, hogy kritikusan megkérdőjelezze a technológia eredményeit. Dokumentálni kell, fel kell mérni és értékelni kell, hogy az emberi felügyelet milyen mértékben változtatja meg az FRT eredeti eredményét.
- Az FRT-modell eltolódásának (teljesítményromlás) nyomon követése és kezelése a modell üzemeltetése során.
- A kockázatok és a biztonsági intézkedések rendszeres, és minden olyan alkalommal történő újraértékelésére irányuló folyamat létrehozása, amikor a technológiában vagy a felhasználási esetben bármilyen változás következik be.
- A rendszerben bekövetkező bármely változás dokumentálása annak teljes életciklusa alatt (pl. korszerűsítés, újratanítás).

- Az érintettek hozzáférési kérelmeinek kezelésére irányuló folyamat, valamint a kapcsolódó technikai funkciók létrehozása. Amennyiben az adatokat az érintettek rendelkezésére kell bocsátani, az adatok kinyeréséhez szükséges technikai kapacitásnak minden kérelem benyújtása előtt rendelkezésre kell állnia.
- Az adatvédelmi incidensekre vonatkozó eljárások rendelkezésre állásának biztosítása A biometrikus adatokat érintő adatvédelmi incidensek esetén a kockázatok valószínűleg magasak lesznek. Ebben az esetben minden érintett felhasználónak tisztában kell lennie a követendő eljárásokkal, az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell, és az érintetteket is tájékoztatni kell.

III. MELLÉKLET – GYAKORLATI PÉLDÁK

Az arcfelismerést számos különböző környezetben, illetve célból használják – ellenőrzött környezetben, mint például határátkelőhelyeken, a rendőrségi adatbázisokból származó vagy az érintett által kifejezetten nyilvánosságra hozott személyes adatokkal való összevetésre, élő kamerafelvételeken (élő arcfelismerés) stb. Ezért a különböző felhasználási esetekben jelentősen eltérnek a személyes adatok és más alapvető jogok és szabadságok védelmét érintő kockázatok. Az arcfelismerés lehetséges alkalmazásáról szóló döntést megelőző szükségességi és arányossági értékelés megkönnyítése érdekében a jelenlegi iránymutatások – példálózó jelleggel – felsorolják az FRT bűnüldözés területén történő lehetséges alkalmazásait.

A bemutatott és értékelt forgatókönyvek **feltételezett** helyzeteken alapulnak és céljuk, hogy bemutassák az FRT bizonyos konkrét alkalmazásait, segítséget nyújtsanak az eseti mérlegeléshez és egy általános keretet határozzanak meg. Nem törekszenek a teljességre és nem érintik a nemzeti felügyeleti hatóságok által az arcfelismerési technológiák kialakítása, kikísérletezése vagy alkalmazása vonatkozásában folytatott vagy tervezett eljárásokat. Ezeknek a forgatókönyveknek az ismertetése csupán azt a célt szolgálja, hogy az arcfelismerő technológiákat kidolgozó és végrehajtását tervező politikai döntéshozók, jogalkotók és bűnüldöző hatóságok számára példákkal illusztrálja az e dokumentumban ismertetett iránymutatásokat, ezáltal biztosítva a személyes adatok védelmére vonatkozó uniós vívmányoknak való teljes körű megfelelést. Ebben az összefüggésben nem szabad azonban elfelejteni, hogy még az FRT hasonló alkalmazása esetén is bizonyos elemek megléte vagy hiánya a szükségesség és arányosság vizsgálatának eltérő kimeneteléhez vezethet.

1 1. FORGATÓKÖNYV

1.1. Leírás

Automatizált határellenőrzési rendszer, amely lehetővé teszi az automatikus határátlépést azáltal, hogy hitelesíti az uniós polgárok és más, a határátkelőhelyen áthaladó utasok elektronikus úti okmányában tárolt biometrikus képet, és megállapítja, hogy az utas az okmány jogos tulajdonosa-e.

Az ilyen ellenőrzés/hitelesítés az arcfelismeréshez csak egy az egyhez megfeleltetést alkalmaz, és ellenőrzött környezetben történik (pl. repülőtéri e-kapuknál). A határátkelőn áthaladó utas biometrikus adatait akkor rögzítik, amikor kifejezetten felszólítják, hogy nézzen az e-kapu kamerájába. Ezután az adatokat összehasonlítják a bemutatott, meghatározott technikai követelmények szerint kiállított okmányban (útlevél, személyazonosító igazolvány stb.) szereplő biometrikus adatokkal.

Ugyanakkor, bár ilyen esetekben az adatkezelés elvben nem tartozik a LED hatálya alá, a határellenőrzés részeként az ellenőrzés eredménye felhasználható a személy (alfanumerikus) adatainak a bűnüldözési adatbázisokkal való összevetésére is, és ezáltal az érintettre nézve jelentős joghatással járó intézkedéseket, pl. a SIS-ben szereplő figyelmeztető jelzés alapján történő letartóztatást vonhat maga után. Bizonyos körülmények fennállása esetén a biometrikus adatok arra is felhasználhatók, hogy egyezéseket keressenek a bűnüldözési adatbázisokban (ilyen esetben ebben a lépésben egy a többhöz megfeleltetésre, azaz azonosításra kerülne sor).

A biometrikus képfeldolgozás eredménye közvetlen hatással van az érintettre: csak sikeres ellenőrzés esetén teszi lehetővé a határátlépést. Sikertelen azonosítás esetén a határőröknek egy második ellenőrzést kell végezniük, hogy megbizonyosodjanak arról, hogy az érintett személy nem azonos az azonosító okmányban szereplő személlyel.

Amennyiben SIS-t vagy nemzeti figyelmeztető jelzést azonosítanak, a határőröknek el kell végezniük egy második ellenőrzést és a szükséges további ellenőrzéseket, majd meg kell tenniük a szükséges intézkedéseket, pl. le kell tartóztatniuk az adott személyt, tájékoztatniuk kell az érintett hatóságokat.

Az információ forrása:

- Az érintettek típusai: ☒ a határokat átlépő valamennyi személy
- A kép forrása: ☒ egyéb (azonosító okmány)
- Bűncselekménnyel fennálló kapcsolat: ☒ Nem szükséges
- Az információgyűjtés módja: ☒ egy fülkében vagy ellenőrzött környezetben.
- Kontextus – más alapvető jogokat érint: Igen, nevezetesen: ☒ a szabad mozgáshoz való jog ☒ menedékjog

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☒ határellenőrzéssel kapcsolatos specifikus adatbázisok.

Algoritmus:

- Az ellenőrzés típusa:☒ egy az egyhez megfeleltetés (hitelesítés)

Eredmény

- Hatás ☒ Közvetlen (az érintettnek engedélyezik vagy megtagadják a belépést)
- Automatizált döntés: ☒ Igen

1.2. Az alkalmazandó jogi keret

A 2252/2004/EK tanácsi rendelet[85] értelmében a tagállamok által kiállított útleveleknek és egyéb úti okmányoknak 2004 óta tartalmazniuk kell egy biometrikus arcképmást, amelyet az okmányba épített elektronikus chipen tárolnak.

A Schengeni határellenőrzési kódex (SBC)[86] meghatározza a külső határokon történő személyellenőrzésre vonatkozó követelményeket. Az uniós polgárok és az uniós jog alapján szabad mozgáshoz való jogot élvező más személyek esetében az úti okmányok minimális, adott esetben technikai eszközök alkalmazásával történő ellenőrzéséből kell állnia. A Schengeni határellenőrzési kódexet az (EU) 2017/2225 rendelettel[87] módosították, amely többek között bevezette az „elektronikus átléptető kapu", az „automatizált határellenőrzési rendszer" és az „önkiszolgáló rendszer" fogalmát, valamint a biometrikus adatok határforgalom-ellenőrzés céljából történő kezelésének lehetőségét.

Ezért feltételezhető, hogy létezik egy egyértelmű és előre látható jogalap, amely engedélyezi a személyes adatok kezelésének e formáját. Emellett a jogi keretet uniós szinten fogadták el, és az közvetlenül alkalmazandó a tagállamokra.

1.3. Szükségesség és arányosság – cél/ a bűncselekmény súlyossága

Az uniós polgárok személyazonosságának automatizált határellenőrzés keretében, biometrikus arcképmásuk felhasználásával történő ellenőrzése az EU külső határain végzett határellenőrzés egyik eleme. Következésképpen közvetlenül kapcsolódik a határbiztonsághoz, és az Unió által elismert közérdekű célt szolgál. Emellett az automatizált határellenőrzési kapuk segítenek felgyorsítani az utasok adatainak kezelését, és csökkentik az emberi hibák kockázatát. Ezen túlmenően a beavatkozás

[85]A Tanács 2004. december 13-i 2252/2004/EK rendelete a tagállamok által kibocsátott útlevelek és úti okmányok biztonsági jellemzőire és biometrikus jellemzőire vonatkozó előírásokról

[86]AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. MÁRCIUS 9-I 2016/399/EU RENDELETE a személyek határátlépésére irányadó szabályok közösségi kódexének (Schengeni határellenőrzési kódex) létrehozásáról

[87] Az Európai Parlament és a Tanács 2017. november 30-i (EU) 2017/2225 rendelete az (EU) 2016/399 rendeletnek a határregisztrációs rendszer alkalmazása tekintetében történő módosításáról

hatóköre, mértéke és intenzitása ebben a forgatókönyvben sokkal korlátozottabb, mint az arcfelismerés más formái esetében. Mindazonáltal a biometrikus adatok kezelése további kockázatokkal jár az érintettek számára, amelyeket az FRT-t üzembe helyező és működtető illetékes hatóságnak megfelelően kezelnie és mérsékelnie kell.

1.4. Következtetés

Az uniós polgárok személyazonosságának az automatizált határellenőrzéssel összefüggésben történő ellenőrzése szükséges és arányos intézkedés mindaddig, amíg megfelelő garanciák vannak érvényben, különös tekintettel a célhoz kötöttség, az adatminőség, az átláthatóság és a magas szintű biztonság elvének alkalmazására.

2 2. FORGATÓKÖNYV

2.1. Leírás

A bűnüldöző hatóságok létrehoznak egy rendszert a gyermekrablás áldozatainak azonosítására. Az erre felhatalmazott rendőr szigorú feltételek mellett elvégezheti a gyaníthatóan elrabolt gyermek biometrikus adatainak a gyermekrablás áldozatainak adatbázisával való összevetését, kizárólag abból a célból, hogy azonosítsa azokat a kiskorúakat, akik megfelelhetnek az eltűnt gyermek leírásának, akivel kapcsolatban nyomozást indítottak és figyelmeztető jelzést adtak ki.

A szóban forgó adatkezelés az egyén arcának vagy arcképmásának – amely megfelelhet egy eltűnt gyermek leírásának – az adatbázisban tárolt képekkel való összehasonlítására terjed ki. Az ilyen adatkezelésre egyedi esetekben, nem pedig szisztematikusan kerül sor.

Az összehasonlítás alapjául szolgáló adatbázist olyan eltűnt gyermekek képeivel töltik fel, akik esetében gyermekrablás gyanúját, a gyermek életét vagy testi épségét fenyegető veszélyt jelentettek be, és akikre vonatkozóan igazságügyi hatóság büntetőeljárást indított, illetve gyermekrablás miatt figyelmeztető jelzést adtak ki. Az adatok gyűjtése az illetékes bűnüldöző hatóság, azaz az igazságügyi rendőri feladatok ellátására felhatalmazott rendőrök által meghatározott eljárások keretében történik. A rögzített személyes adatok kategóriái a következők:

- személyazonosság, becenév, álnév, leszármazás, állampolgárság, címek, e-mail címek, telefonszámok;
- születési hely és idő;
- szülői információk;
- arcfelismerő eszköz használatát lehetővé tevő műszaki jellemzőkkel rendelkező fénykép és más fényképek.

Az összehasonlítás eredményeit egy erre felhatalmazott tisztviselőnek is felül kell vizsgálnia és ellenőriznie kell annak érdekében, hogy a korábbi bizonyítékokat alátámassza az összehasonlítás eredményével, és kizárja az esetleges hibás egyezéseket.

A gyermekek fényképei és személyes adatai csak a figyelmeztető jelzés időtartama alatt őrizhetők meg, és azokat a büntetőeljárás lezárását vagy befejezését követően haladéktalanul törölni kell azon nemzeti eljárásoknak megfelelően, amelyek vonatkozásában az adatbázisba kerültek.

Míg a biometrikus adatok adatbázisban való megőrzésének időtartamát viszonylag hosszú időtartamra lehet előirányozni, és azt a nemzeti jog határozza meg, az érintettek jogainak és különösen a

helyesbítéshez és törléshez való jogának gyakorlása további garanciát nyújt az érintettek személyes adatok védelméhez való jogába való beavatkozás korlátozására.

Az információ forrása:

- Az érintettek típusai:☒ Gyermekek
- A kép forrása ☒ egyéb: nem előre meghatározott, gyermekrablás feltételezett áldozata
- Bűncselekménnyel fennálló kapcsolat ☒ Nem közvetlen időbeli ☒ Nem közvetlen földrajzi
- Az információgyűjtés módja: ☒ egy fülkében vagy ellenőrzött környezetben.
- Kontextus: más alapvető jogokat érint ☒ Igen, nevezetesen: ☒ több alapvető jog

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság ☒ specifikus adatbázis

Algoritmus:

- Az ellenőrzés típusa:☒ azonosítás (egy a többhöz megfeleltetés)

Eredmény

- Hatás ☒ Közvetlen
- Automatizált döntés: ☒ NEM, kötelező felülvizsgálat egy felhatalmazott tisztviselő által

Jogi elemzés:

- Alkalmazandó jogi keret:☒ Az ilyen adatkezelésre (arcfelismerés) vonatkozó konkrét nemzeti jogszabály

2.2. Az alkalmazandó jogi keret

A nemzeti jog külön jogi keretet biztosít az adatbázis létrehozására, amely meghatározza az adatkezelés céljait, valamint az adatbázis feltöltésének, hozzáférhetőségének és használatának kritériumait. A végrehajtásához szükséges jogalkotási intézkedések az adatmegőrzési időszak meghatározásáról is rendelkeznek, valamint hivatkoznak az integritás és bizalmas jelleg alkalmazandó elveire. A jogalkotási intézkedések rendelkeznek az érintett, és ebben az esetben a szülői felelősség gyakorlója (gyakorlói) részére történő információszolgáltatás módjáról, valamint az érintettek jogainak gyakorlásáról és adott esetben a lehetséges korlátozásról is. Az adott jogalkotási intézkedésre vonatkozó javaslat előkészítése során konzultálni kell a nemzeti felügyeleti hatósággal.

2.3. Szükségesség és arányosság – cél/a bűncselekmény súlyossága/a bűncselekményben nem érintett, de az adatkezelés által érintett személyek száma

Az adatkezelés feltételei és garanciái

Az arcfelismerés segítségével történő összehasonlítást az erre felhatalmazott tisztviselő csak végső esetben végezheti el, ha nem áll rendelkezésre más, kevésbé beavatkozó eszköz és ha az feltétlenül szükséges, például abban az esetben, ha kétség merül fel egy utazó kiskorú személyazonosító okmányának hitelességével kapcsolatban és/vagy miután áttekintette egy olyan eltűnt gyermek személyleírásával való lehetséges egyezésre utaló korábbi bizonyítékokat és összegyűjtött anyagokat, akivel kapcsolatban nyomozás folyik.

További garanciát jelent az arcfelismerés felhatalmazott tisztviselő általi kötelező felülvizsgálata és ellenőrzése annak érdekében, hogy a korábbi bizonyítékokat alátámasszák az összehasonlítás eredményével, és ki lehessen zárni az esetleges hibás egyezéseket.

A kitűzött cél

Az adatbázis létrehozása fontos általános közérdekű célokat, különösen a bűncselekmények megelőzését, nyomozását, felderítését, a vádeljárás lefolytatását vagy büntetőjogi szankciók végrehajtását, valamint mások jogainak és szabadságainak védelmét szolgálja. Az adatbázis létrehozása és a tervezett adatkezelés feltehetően hozzájárul a gyermekrablás áldozatául esett gyermekek azonosításához, ezért olyan intézkedésnek tekinthető, amely alkalmas az ilyen bűncselekmények kivizsgálására és a büntetőeljárás alá vonás mint jogszerű célkitűzés támogatására.

Az adatbázis célja és populációja

Az adatkezelés céljait a jogszabályok egyértelműen meghatározzák, és az adatbázis csak olyan eltűnt gyermekek azonosítása céljából használható, akik esetében gyermekrablás gyanúját jelentették és igazságügyi hatóság felügyelete mellett nyomozást indítottak, valamint gyermekrablásra vonatkozó figyelmeztető jelzést adtak ki. A jogszabályban az adatbázis populációjára vonatkozóan meghatározott feltételek célja, hogy szigorúan korlátozzák az adatbázisba felveendő érintettek és személyes adatok számát. A gyermek feletti szülői felelősség gyakorlóját tájékoztatni kell az adatkezelésről és az azonosítás céljából tervezett biometrikus adatkezeléssel, vagy a gyermek adatbázisban tárolt személyes adataival kapcsolatos jogainak gyakorlására vonatkozó feltételekről.

2.4. Következtetés

Figyelembe véve a tervezett adatkezelés szükségességét és arányosságát, valamint a gyermeknek az ilyen személyesadat-kezelés elvégzéséhez fűződő legjobb érdekét, és feltéve, hogy megfelelő garanciák állnak rendelkezésre annak biztosítására, hogy az érintettek gyakorolhassák jogaikat – különösen figyelembe véve, hogy gyermekek adatait kell feldolgozni –, az arcfelismerés segítségével történő adatkezelés ilyen alkalmazása valószínűleg összeegyeztethetőnek tekinthető az uniós joggal.

Figyelemmel továbbá az adatkezelés típusára és az alkalmazott technológiára, amely az érintett jogaira és szabadságaira nézve magas kockázattal jár, az Európai Adatvédelmi Testület úgy véli, hogy a tervezett adatkezelésre vonatkozó, a nemzeti parlament által elfogadandó jogalkotási intézkedésre irányuló javaslat, vagy az ilyen jogalkotáson alapuló szabályozási intézkedés előkészítése során előzetes konzultációt kell folytatni a felügyeleti hatósággal az alkalmazandó jogi keretnek való megfelelés, és annak betartása érdekében, vö. a LED 28. cikkének (2) bekezdése.

3 3. FORGATÓKÖNYV

3.1. Leírás

A zavargások és az azokat követő nyomozások alkalmával végzett rendőrségi beavatkozások során számos személyt gyanúsítottként azonosítottak, például CCTV-felvételeket vagy tanúkat felhasználó korábbi nyomozások alapján. A gyanúsítottak képeit összehasonlítják a bűncselekmény helyszínén vagy annak környékén CCTV vagy mobilkészülékek által rögzített személyek képeivel.

Annak érdekében, hogy részletesebb bizonyítékokat szerezzenek a tüntetést övező zavargásokban való részvétellel gyanúsított személyekről, a rendőrség képanyagokat tartalmazó adatbázist hoz létre, amely laza helyi és időbeli kapcsolatban áll a zavargásokkal. Az adatbázis tartalmazza a polgárok által a rendőrség honlapjára feltöltött magánfelvételeket, a tömegközlekedési eszközök CCTV-inek anyagát, a rendőrség tulajdonában lévő videó megfigyelési anyagokat, és a média által minden különösebb korlátozás vagy garancia nélkül közzétett anyagokat. A súlyos bűnöző magatartás tanúsítása nem előfeltétele a fájlok adatbázisban való gyűjtésének. Ezért olyan személyek is bekerülnek az adatbázisba, akik nem vettek részt a zavargásokban, így például a helyi lakosság jelentős százaléka,

akik a tüntetés idején a közelben tartózkodtak vagy részt vettek ugyan a tüntetésen, de a zavargásokban nem. Ez több ezer videó- és képfájlt jelent.

Az arcfelismerő szoftver segítségével az ezekben a fájlokban megjelenő valamennyi arcot egyedi arcazonosítóhoz rendelik, majd az egyes gyanúsítottak arcképmásait automatikusan összevetik ezekkel az arcazonosítókkal. A több ezer videó- és képfájlban található valamennyi biometrikus sablont tartalmazó adatbázist addig tárolják, amíg minden lehetséges nyomozás le nem zárul. A pozitív találatokkal felelős tisztviselők foglalkoznak, akik ezután döntenek a további intézkedésekről. Ezek magukban foglalhatják az adatbázisban található fájlnak az adott személy bűnügyi aktájához való hozzárendelését, valamint olyan további intézkedéseket, mint az adott személy kihallgatása vagy letartóztatása.

A nemzeti jogszabály általános rendelkezést tartalmaz, amely szerint a biometrikus adatoknak egy természetes személy egyedi azonosítása céljából történő feldolgozása akkor megengedett, ha az feltétlenül szükséges, és az érintett személy jogaira és szabadságaira vonatkozó megfelelő garanciák mellett történik.

Az információ forrása:

- Az érintettek típusai: ☒ valamennyi személy
- A kép forrása: ☒ nyilvános terek ☒ magánszervezet ☒ egyéb magánszemélyek ☒ egyéb: média
- Bűncselekménnyel fennálló kapcsolat: ☒ Nem feltétlenül közvetlen földrajzi vagy időbeli kapcsolat
- Az információgyűjtés módja: ☒ távoli
- Kontextus – más alapvető jogokat érint: Igen, nevezetesen ☒ a gyülekezési szabadság
- Az érintettre vonatkozóan rendelkezésre álló további információforrások:
  ☒ egyéb: nem kizárt (pl. ATM-gépek használata vagy látogatott üzletek), mivel a képeken szereplő motívumok nem ellenőrizhetők

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☒ a bűnözéssel kapcsolatos specifikus adatbázisok

Algoritmus:

- Az adatkezelés típusa: ☒ azonosítás (egy a többhöz megfeleltetés)

Eredmény

- Hatás: ☒ Közvetlen (pl. az érintett letartóztatható, kihallgatható)
- Automatizált döntés: ☒ NEM
- Az adattárolás időtartama: az összes lehetséges vizsgálat befejezéséig

Jogi elemzés:

- Az érintett előzetes tájékoztatásának típusa: ☒ A bűnüldöző hatóság honlapján található általános információk
- Alkalmazandó jogi keret: A☒ LED nagyrészben a nemzeti jogba átültetve☒ A biometrikus adatok bűnüldöző hatóságok általi használatára vonatkozó általános nemzeti jogszabály

3.2. Az alkalmazandó jogi keret

A fentebb leírtak szerint a LED 10. cikkének általános rendelkezését csak megismétlő jogalapok nem elég egyértelműek ahhoz, hogy az egyének számára megfelelő tájékoztatást nyújtsanak azokról a feltételekről és körülményekről, amelyek fennállása esetén a bűnüldöző hatóságok jogosultak nyilvános térben készült CCTV-felvételeket felhasználni az arcuk biometrikus sablonjának

elkészítéséhez, illetve azoknak a rendőrségi adatbázisokkal vagy más rendelkezésre álló CCTV- vagy magánfelvételekkel történő összehasonlításához. Az ebben a forgatókönyvben megállapított jogi keret tehát nem felel meg a jogalapra vonatkozó minimum követelményeknek.

3.3. Szükségesség és arányosság

Ebben a példában az adatkezelés a szükségesség és arányosság elve vonatkozásában több okból is számos aggályt vet fel:

A személyeket nem gyanúsítják súlyos bűncselekmény elkövetésével. A súlyos bűnözői magatartás tanúsítása nem előfeltétele a képanyagot tartalmazó adatbázisban található fájlok felhasználásának. Emellett a bűncselekménnyel való közvetlen időbeli és földrajzi kapcsolat sem előfeltétele az adatbázisban tárolt fájlok felhasználásának. Ez azt eredményezi, hogy a helyi lakosság jelentős hányadának arcképmásait potenciálisan több évig, az összes vizsgálat lezárásáig biometrikus adatbázisban tárolják.

A bűnügyi helyszínre vonatkozó adatbázisban nem csak az arányossági követelményeknek megfelelő képek találhatók, aminek eredményeképpen korlátlan számú összehasonlítandó kép áll rendelkezésre. Ez ellentmond az adattakarékosság elvének. A képek kisebb mennyisége lehetővé tenné nem-algoritmikus és kevésbé beavatkozó jellegű eszközök (pl. szuperfelismerők) alkalmazásának mérlegelését is.[88]

Mivel a példa egy tüntetés környezetére vonatkozik, valószínű, hogy a képek a tüntetés résztvevőinek politikai véleményét is felfedik, amely az e forgatókönyv által esetlegesen érintett adatok második különleges kategóriáját jelenti. Ebben a forgatókönyvben nem világos, hogyan és milyen garanciák mellett akadályozható meg ezen adatok gyűjtése. Továbbá, ha az érintettek megtudják, hogy egy tüntetésben való részvételük biometrikus rendőrségi adatbázisba való felvételüket eredményezte, ez komoly elrettentő hatással lehet a gyülekezéshez való joguk jövőbeli gyakorlására.

Az adatbázisban található biometrikus sablonok is összehasonlíthatók egymással. Ez lehetővé teszi a rendőrség számára, hogy ne csak egy adott személyt keressen az összes anyagban, hanem egy személy viselkedési mintáját több napon keresztül újra létrehozza. További információkat is gyűjthet a személyekről, például a társadalmi kapcsolataikkal és politikai részvételükkel kapcsolatban.

A beavatkozás súlyosságát tovább fokozza az a tény, hogy az adatok kezelése az érintettek tudta nélkül történik.

Ha figyelembe vesszük, hogy az emberek egész idő alatt készítenek fényképeket és videófelvételeket, és hogy még a mindenütt jelenlévő CCTV-k felvételei is biometrikusan elemezhetők, ez komoly elrettentő hatással járhat.

Szintén aggodalomra ad okot a magánjellegű fényképek és videók széles körű használata, beleértve az ezzel kapcsolatos esetleges visszaéléseket (például a feljelentés) is. Mivel a büntetőeljárások általában már eleve magukban hordozzák a feljelentéshez hasonló visszaélések kockázatát, az adatok skálázhatóságát és az érintett személyek számát tekintve lényegesen nagyobb a kockázat, mivel az emberek egy ellenszenves személyre vagy személycsoportra vonatkozó anyagot is feltölthetnek. A rendőrség fényképek és videók feltöltésére irányuló felhívásai nagyon alacsony küszöböket

[88] Azaz rendkívüli arcfelismerő képességgel rendelkező személyek. Vö. továbbá: Face Recognition by Metropolitan Police Super-Recognisers, 2016 Feb 26, DOI:10.1371/journal.pone.0150036,2016https://pubmed.ncbi.nlm.nih.gov/26918457/

eredményezhetnek az anyagok rendelkezésre bocsátására vonatkozóan, különösen azért, mert ez névtelenül vagy legalábbis a rendőrségen való személyes megjelenés és a személyazonosság igazolása nélkül is lehetséges.

3.4. Következtetés

A példában nincsen olyan konkrét rendelkezés, amely jogalapként szolgálhatna. Azonban még ha lenne is megfelelő jogalap, a szükségesség és az arányosság követelménye nem teljesülne, ami aránytalan beavatkozást eredményez az érintetteknek a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő, a Chartában megfogalmazott jogaiba.

4 4. FORGATÓKÖNYV

4.1. Leírás

A rendőrség a súlyos bűncselekményt elkövető gyanúsítottakat CCTV-kamerák felvételei alapján, retrospektív arcfelismerő technológia segítségével azonosítja. Egy tisztviselő manuálisan kiválasztja a gyanúsítottak képét/képeit a bűnügyi helyszínen vagy az előzetes nyomozás során máshol gyűjtött videóanyagból, majd elküldi azokat a kriminalisztikai osztálynak. A kriminalisztikai osztály az FRT-t arra használja, hogy ezeket a képeket összevesse személyeknek a rendőrség által korábban egy adatbázisban összegyűjtött képeivel (úgynevezett leíró adatbázis, amely gyanúsítottak és korábbi elítéltek adatait tartalmazza). A leíró adatbázist ennek az eljárásnak a vonatkozásában – ideiglenesen és elszigetelt környezetben – FRT-vel kell elemezni annak érdekében, hogy végre lehessen hajtani az összevetési folyamatot. A személyes adatok összevetésével érintett személyek jogaiba és érdekeibe való beavatkozás minimalizálása érdekében a kriminalisztikai osztályon csak nagyon korlátozott számú alkalmazottnak van engedélye a tényleges összevetés lefolytatására, az adatokhoz való hozzáférés az adott ügyirattal megbízott tisztviselőkre korlátozódik, és az eredményeket manuálisan ellenőrzik, mielőtt bármilyen eredményt továbbítanának a nyomozó tisztviselőnek. A biometrikus adatokat nem az ellenőrzött, elszigetelt környezeten kívül továbbítják. A vizsgálat során kizárólag az eredményt és a képet (nem a biometrikus sablont) használják tovább. Az alkalmazottak külön képzésben részesülnek az ilyen adatkezelés szabályairól és eljárásairól, és a személyes és biometrikus adatok kezelése a nemzeti jogban megfelelően szabályozott.

Az információ forrása:

- Az érintettek típusai: ☒ CCTV-kamerák felvételein azonosított gyanúsítottak
- A kép forrása: ☒ nyilvános terek☒ internet
- Bűncselekménnyel fennálló kapcsolat:☒ Közvetlen időbeli
  ☒ Közvetlen földrajzi
- Az információgyűjtés módja: ☒ távoli
- Egyéb alapvető jogokat érintő kontextus: Igen, nevezetesen: ☒ A gyülekezés szabadsága ☒ A véleménynyilvánítás szabadsága ☒ más: __

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☒ a bűnözéssel kapcsolatos specifikus adatbázisok

Algoritmus:

- Az adatkezelés típusa: ☒ azonosítás (egy a többhöz megfeleltetés)

Eredmény

- Hatás: ☒ Közvetlen (pl. az érintettet letartóztatják, kihallgatják)
- Automatizált döntés: ☒ NEM

Jogi elemzés:

- Alkalmazandó jogi keret:☒ Az ilyen adatkezeléssel (arcfelismerés) kapcsolatban az adott illetékes hatóságra vonatkozó, konkrét nemzeti jogszabály

4.2. Az alkalmazandó jogi keret

Ebben az esetben a nemzeti jog előírja, hogy a biometrikus adatok akkor használhatók fel kriminalisztikai elemzések elvégzésére, ha ez feltétlenül szükséges ahhoz, hogy a súlyos bűncselekményt elkövető gyanúsítottakat a leírási adatbázisban szereplő képekkel való összevetés révén azonosítani lehessen. A nemzeti jog meghatározza a kezelhető adatok típusát, a személyes adatok sértetlenségének és titkosságának megőrzésére szolgáló eljárásokat, valamint a megsemmisítésükre szolgáló eljárásokat, így elegendő garanciát nyújt a visszaélés és az önkényesség kockázatával szemben.

4.3. Szükségesség és arányosság

Az arcfelismerés használata egyértelműen időhatékonyabb, mint a kriminalisztika által végzett manuális összevetés. A képek előzetes manuális kiválasztása korlátozza a beavatkozást az összes videóanyag adatbázissal történő összevetéséhez képest, és ezáltal csak a célkitűzés, azaz a súlyos bűncselekmények elleni küzdelemmel érintett személyeket különbözteti és célozza meg. Mindazonáltal továbbra is fontos mérlegelni, hogy az adott esetben az adatok összevetése észszerű időn belül elvégezhető-e manuálisan. A technológiához és a személyes adatokhoz hozzáféréssel rendelkező személyek korlátozása, valamint az a gyakorlat, hogy a biometrikus sablonokat nem tárolják, illetve használják fel később a nyomozás során, csökkenti a magánélethez és az adatvédelemhez való jogra gyakorolt hatást. Az eredmény manuális ellenőrzése azt is jelenti, hogy csökken a hibás egyezések kockázata.

4.4. Következtetés

Fontos, hogy a nemzeti jogszabályok megfelelő jogalapot biztosítsanak a biometrikus adatok kezelésével, valamint azzal a nemzeti adatbázissal kapcsolatban, amellyel az adatokat összevetik. E forgatókönyv alapján számos intézkedést vezettek be az adatvédelmi jogokba való beavatkozás korlátozása érdekében, ilyen például az FRT használatának a jogalap során meghatározott feltételei, a technológiához és a biometrikus adatokhoz hozzáféréssel rendelkező személyek száma, manuális ellenőrzések stb. Az FRT jelentős mértékben növeli a rendőrség kriminalisztikai osztálya által végzett nyomozás hatékonyságát, olyan jogszabályon alapul, amely a rendőrség számára abban az esetben teszi lehetővé, hogy biometrikus adatokat dolgozzon fel, ha az feltétlenül szükséges, és ezért e kereteken belül az egyén jogaiba való jogszerű beavatkozásnak tekinthető.

5 5. FORGATÓKÖNYV

5.1. Leírás

A távoli biometrikus azonosítás azt jelenti, hogy a személyek azonosságát biometrikus azonosítók (arcképmás, járás, írisz stb.) segítségével távolról, nyilvános térben és folyamatos jelleggel, az adatbázisban tárolt (biometrikus) adatokkal való összevetés útján állapítják meg[89]. A távoli biometrikus

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

azonosításra valós időben kerül sor, ha a képanyag rögzítése, az összehasonlítás és az azonosítás jelentős késedelem nélkül történik.

A valós idejű távoli biometrikus azonosítás minden egyes üzembe helyezése előtt a rendőrség a nyomozás részeként figyelőlistát állít össze az érdeklődésre számot tartó személyekről. A figyelőlistára az egyének arcképmása kerül. Olyan hírszerzési adatok alapján, amelyek arra utalnak, hogy az egyének egy adott területen – például egy bevásárlóközpontban vagy valamely nyilvános térben – fognak tartózkodni, a rendőrség eldönti, hogy mikor, hol és mennyi ideig alkalmazza a távoli biometrikus azonosítást.

Az akció napján a helyszínen egy rendőrségi furgont helyeznek el irányító központként, egy vezető rendőrtiszttel a fedélzeten. A furgonban olyan monitorok vannak, amelyek a közelben elhelyezett CCTV-kamerák felvételeit mutatják, amelyeket vagy eseti alapon telepítettek, vagy a már telepített kamerák videó folyamaihoz csatlakoznak. Ahogy a gyalogosok elhaladnak a kamerák előtt, a technológia elkülöníti az arcképmásokat, azokat biometrikus sablonná alakítja, majd összehasonlítja a figyelőlistán szereplő személyek biometrikus sablonjaival.

A figyelőlista és a kamerák előtt elhaladó személyek között potenciális egyezés esetén a furgonban lévő rendőrök riasztást kapnak, akik aztán pozitív találat estén, például rádión keresztül tájékoztatják a helyszínen lévő rendőröket. A helyszínen tartózkodó rendőr ezután dönt arról, hogy beavatkozik, megközelíti, vagy végső esetben elfogja-e az illetőt. A tisztviselő által a helyszínen hozott intézkedéseket rögzítik. Rejtett ellenőrzés esetén az összegyűjtött információkat (például hogy kivel van a személy, mit viselnek és hová mennek) tárolják.

A hivatkozott nemzeti jogszabály általános rendelkezést tartalmaz, amely szerint a biometrikus adatok feldolgozása egy természetes személy egyedi azonosítása céljából akkor megengedett, ha az feltétlenül szükséges, és az érintett személy jogaira és szabadságaira vonatkozó megfelelő garanciák mellett történik.

Az információ forrása:

- Az érintettek típusai: ☒ valamennyi személy
- A kép forrása: ☒ nyilvános terek
- Bűncselekménnyel fennálló kapcsolat: ☒ Nem feltétlenül közvetlen földrajzi vagy időbeli kapcsolat
- Az információgyűjtés módja: ☒ távoli
- Egyéb alapvető jogokat érintő kontextus: Igen, nevezetesen: ☒ A gyülekezés szabadsága ☒ A véleménynyilvánítás szabadsága ☒ más alapvető jog
- Az érintettre vonatkozóan rendelkezésre álló további információforrások: ☒ egyéb: nem kizárt (pl. ATM-gépek használata vagy látogatott boltok)

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☒ a bűnözéssel kapcsolatos specifikus adatbázisok

Algoritmus:

- Az adatkezelés típusa: ☒ azonosítás (egy a többhöz megfeleltetés)

Eredmény

- Hatás:☒ Közvetlen (pl. az érintettet letartóztatják, kihallgatják)
- Automatizált döntés: ☒ NEM
- Az adattárolás időtartama: az összes lehetséges vizsgálat befejezéséig

Jogi elemzés:

- Az érintett előzetes tájékoztatásának típusa: ☒ A bűnüldöző hatóság honlapján általánosan
- Alkalmazandó jogi keret: A ☒ LED nagyrészben a nemzeti jogba átültetve ☒ A biometrikus adatok bűnüldöző hatóságok általi használatára vonatkozó általános nemzeti jogszabály

5.2. Az alkalmazandó jogi keret

A LED 10. cikkének általános rendelkezését csak megismétlő jogalapok nem elég egyértelműek ahhoz, hogy az egyének számára megfelelő tájékoztatást nyújtsanak azokról a feltételekről és körülményekről, amelyek fennállása esetén a bűnüldöző hatóságok jogosultak nyilvános térben készült CCTV-felvételeket felhasználni az arcuk biometrikus sablonjának elkészítéséhez, illetve azoknak a rendőrségi adatbázisokkal történő összehasonlításához. Az ebben a forgatókönyvben megállapított jogi keret tehát nem felel meg a jogalapra vonatkozó minimum követelményeknek.[90]

5.3. Szükségesség és arányosság

A szükségesség és az arányosság követelménye annál magasabb, minél súlyosabb a beavatkozás. A nyilvános térben történő távoli biometrikus azonosításnak számos alapjogi vonatkozása van:

A forgatókönyvek értelmében az adott nyilvános térben minden járókelőt nyomon kell követni, ezért súlyosan érinti a lakosságnak a nyilvános térben való anonimitáshoz fűződő ésszerű elvárásait[91]. Ez előfeltétele a demokratikus folyamat számos aspektusának, például az arra vonatkozó döntésnek, hogy valaki csatlakozzon-e egy polgári egyesülethez, ellátogasson-e összejövetelekre és találkozzon-e különféle társadalmi és kulturális hátterű emberekkel, részt vegyen-e politikai tiltakozáson és ellátogasson-e különböző helyszínekre. Az anonimitás fogalma a nyilvános terekben elengedhetetlen az információk és ötletek szabad gyűjtéséhez és cseréjéhez. Biztosítja a vélemények sokféleségét, a békés gyülekezés és az egyesülés szabadságát, a kisebbségek védelmét, valamint támogatja a hatalmi ágak szétválasztásának elvét, és a fékek és ellensúlyok rendszerét. Az anonimitás aláásása a nyilvános térben komoly elrettentő hatással lehet a polgárokra. Elképzelhető, hogy tartózkodni fognak a szabad és nyitott társadalomban elfogadott magatartásoktól. Ez kihatna a közérdekre, mivel egy demokratikus társadalomban elengedhetetlen a polgárok önrendelkezése és a demokratikus folyamatban való részvétele.

Ha egy ilyen technológia alkalmazásra kerül, az utcán, a metróállomáshoz vagy a pékségbe tett egyszerű séta a személyes-, többek között biometrikus adatok bűnüldöző szervek általi gyűjtéséhez – és az első forgatókönyv szerint a rendőrségi adatbázisokkal való összevetéshez is – vezet. Amennyiben ugyanezt ujjlenyomat vétel útján tennék, egyértelműen aránytalan lenne .

Az érintettek száma rendkívül magas, mivel mindenki érintett, aki az adott nyilvános térben elsétál. A forgatókönyvek továbbá a biometrikus adatok automatizált tömeges feldolgozását, valamint a biometrikus adatok rendőrségi adatbázisokkal való tömeges összevetését vonnák maguk után.

Az európai ítélkezési gyakorlat szerint tilos a tömeges megfigyelés (pl. az EJEB az S. és Marper kontra Egyesült Királyság ügyben a biometrikus adatok válogatás nélküli megőrzését a magánélethez való

[90]Azokban az esetekben, amikor az FRT használatának kutatására irányuló tudományos projekt keretében személyes adatok kezelésére kerülne sor, de az ilyen adatkezelés nem tartozna a LED 4. cikke (3) bekezdésének vagy az uniós jognak a hatálya alá, a GDPR lenne alkalmazandó. Olyan kísérleti projektek esetében, amelyeket bűnüldözési műveletek követnének, a LED továbbra is alkalmazandó lenne.

[91] Az Európai Adatvédelmi Testület válasza az európai parlamenti képviselőknek a Clearview AI által kifejlesztett arcfelismerő alkalmazással kapcsolatban, 2020. június 10., Hiv.: OUT2020-0052.

jogba történő „aránytalan beavatkozásának” tekintette, mivel az nem tekinthető „egy demokratikus társadalomban szükségesnek”).

A távoli biometrikus azonosítás olyan mértékű tömeges megfigyeléssel jár, amelyet nem lehet megbízható eszközökkel korlátozni. Ez alapvetően különbözik a magától a videó megfigyeléstől, mivel míg a videófelvételek biometrikus azonosítás nélküli lehetséges felhasználása már eleve súlyos, de ugyanakkor korlátozott beavatkozás, addig az FRT alkalmazása esetén a már széles körben elterjedt videó megfigyelési rendszer mint fő adatforrás minőségi változáson megy keresztül. Ezen túlmenően, különösen a feltételezett elrettentő hatás tekintetében, a már meglévő videókamerás megfigyelő berendezések alkalmazásának lehetséges korlátozásai nem lesznek láthatóak, és így a nyilvánosság nem bízik bennük.

A rendőrség által végzett távoli biometrikus azonosítás mindenkit potenciális gyanúsítottként kezel. Egy jogállamban azonban az állampolgárokat mindaddig ártatlannak tekintik, amíg a helytelen magatartás nem bizonyítható. Ez az elv részben tükröződik a LED-ben is, amely hangsúlyozza, hogy amennyire lehetséges, különbséget kell tenni az elítéltek vagy a gyanúsítottak – akik esetében a bűnüldöző hatóságok „*alapos okkal feltételezik, hogy bűncselekményt követtek el vagy készülnek elkövetni*” (a LED 6. cikkének a) pontja) – személyes adatai és azon személyek személyes adatai között, akiket nem ítéltek el vagy nem gyanúsítanak bűncselekmény elkövetésével.

A közlekedési csomópontokon vagy nyilvános térben alkalmazva a bűnüldöző szervek olyan technológiát használnak, amely képes egyetlen személy egyedi azonosítására, valamint tartózkodási helyének és mozgásának nyomon követésére és elemzésére, és amely akár a legérzékenyebb információkat (akár szexuális preferenciák, vallás, egészségügyi problémák) is feltárja egy személyről. Ezzel együtt jár az adatokhoz való jogellenes hozzáférés és felhasználás óriási kockázata.

Egy olyan rendszer telepítése, amely lehetővé teszi az egyén alapvető viselkedésének és jellemzőinek feltárását, jelentős elrettentő hatással jár. Az embereket elbizonytalanítja abban, hogy csatlakozzanak-e egy tüntetéshez, ami veszélyezteti a demokratikus folyamatot. Az is kritikus lehet, ha valaki egy olyan barátjával találkozik vagy mutatkozik nyilvános helyen, akinek gondjai vannak a rendőrséggel, vagy furcsán viselkedik, hiszen az adott személy ezáltal a rendszer algoritmusának, és így a bűnüldöző hatóságoknak a figyelmébe kerülhet.

Az olyan sérülékeny érintetteket, mint a gyermekek, lehetetlen megvédeni. Ezenkívül azok a személyek is érintettek, akiknek szakmai érdeke – és gyakran ennek megfelelő jogi kötelezettsége is –, hogy kapcsolataikat bizalmasan kezeljék, mint például az újságírók, az ügyvédek és a lelkészek. Ez például a adatforrást jelentő személy és az újságíró, vagy annak a ténynek a felfedéséhez vezethet, hogy egy személy büntetőjogi ügyvéddel konzultál. A probléma nemcsak a véletlenszerű nyilvános helyekre vonatkozik, ahol például az újságírók és adatforrásaik találkoznak, hanem természetesen azokra a nyilvános terekre is, amelyek az intézmények vagy szakemberek megközelítéséhez és hozzáféréséhez ebben a vonatkozásban szükségesek.

Ezen túlmenően az FRT-vel kapcsolatos kellemetlen érzések arra késztethetik az embereket, hogy megváltoztassák viselkedésüket, elkerüljék azokat a helyeket, ahol az FRT-t alkalmazzák, és így kivonuljanak a társadalmi életből és a kulturális eseményekből. Az FRT alkalmazásának mértékétől függően az emberekre gyakorolt hatás olyan jelentős lehet, hogy befolyásolja a méltóságteljes életre való képességüket[92].

[92] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, 20. oldal.

Nagy a valószínűsége ezért annak, hogy a személyes adatok védelméhez való jog lényege – az érinthetetlen magja – érintett. Az erre utaló egyértelmű jelek (lásd az iránymutatás 3.1.3.2. pontja) különösen a következők: emberek egyedi biológiai jellemzőinek valószínűségen alapuló algoritmusokkal történő, nagy léptékű automatikus feldolgozása a bűnüldöző hatóságok által az eredmények csak korlátozott megmagyarázhatósága mellett. A magánélet tiszteletben tartásához és a személyes adatok védelméhez való jog korlátozását az adott személy egyéni magatartásától vagy az őt érintő körülményektől függetlenül alkalmazzák. Statisztikailag az e beavatkozással érintett adatalanyok szinte mindegyike törvénytisztelő személy. Az érintett tájékoztatására csak korlátozott lehetőségek állnak rendelkezésre. A bírósági jogorvoslat a legtöbb esetben csak utólag lesz lehetséges.

A valószínűségen alapuló és korlátozott megmagyarázhatósággal rendelkező rendszerre való támaszkodás a felelősség diffúziójához és a jogorvoslattal kapcsolatos hiányossághoz vezethet, valamint gondatlanságra ösztönözhet.

Amennyiben egy ilyen, már meglévő CCTV-kamerákra is alkalmazható rendszer alkalmazásra kerül, azzal – nagyon kis erőfeszítéssel és anélkül, hogy az egyének számára látható lenne – vissza lehet élni, és segítségével szisztematikusan és gyorsan listákat lehet összeállítani az emberekről etnikai származás, nem, vallás stb. alapján. A személyes adatok előre meghatározott kritériumok – mint például a személy tartózkodási helye és a megtett útvonal – alapján történő kezelésének elvét már alkalmazzák[93], és fennáll a diszkrimináció lehetősége.

A kezelt adatok érzékenysége, kifejezőereje és mennyisége miatt a nyilvános térben alkalmazott távoli arcfelismerő rendszerekkel vissza lehet élni, ami káros hatásokkal lehet az érintett személyekre. Az ilyen adatok könnyen gyűjthetők és könnyű velük abból a célból visszaélni, hogy nyomást gyakoroljanak a fékek és ellensúlyok rendszerének kulcsszereplőire, például a politikai ellenzékre, a tisztségviselőkre és az újságírókra.

Végül, az FRT-rendszerek a faji és nemi hovatartozás tekintetében általában torzítanak: a hibás egyezések aránytalanul nagy mértékben érintik a színesbőrűeket és a nőket[94], ami diszkriminációt eredményez. A hibás egyezést követő rendőrségi intézkedések, mint például a házkutatások és a letartóztatások, még jobban megbélyegzik ezeket a csoportokat.

5.4. Következtetés

A biometrikus adatok nyilvános térben történő, azonosítási célú távoli feldolgozására vonatkozó fent leírt forgatókönyvek nem állítanak fel méltányos egyensúlyt az egymással versengő magán- és közérdekek között, ezért aránytalan beavatkozást jelentenek az érintetteknek a Charta 7. és 8. cikke szerinti jogaiba.

[93] Vö. Az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról szóló, 2016. április 27-i (EU) 2016/681 európai parlamenti és tanácsi irányelv 6. cikke, valamint az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról, valamint az 1077/2011/EU rendelet, az 515/2014/EU rendelet, az (EU) 2016/399 rendelet, az (EU) 2016/1624 rendelet és az (EU) 2017/2226 rendelet módosításáról szóló, 2018. szeptember 12-i (EU) 2018/1240 európai parlamenti és tanácsi rendelet 33. cikke.

[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf,
http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

6 6. FORGATÓKÖNYV

6.1. Leírás

Egy magánszervezet olyan alkalmazást nyújt be, amelyben az arcképmásokat az internetről gyűjtötték adatbázis létrehozása céljából. A felhasználó, pl. a rendőrség, feltölthet egy képet, amelyet az alkalmazás biometrikus azonosítás segítségével megpróbál összevetni az adatbázisában található arcképmásokkal vagy biometrikus sablonokkal.

Egy helyi rendőrkapitányság nyomozást folytat egy videóra vett bűncselekmény ügyében, ahol számos lehetséges tanút és gyanúsítottat nem lehet azonosítani az összegyűjtött információk belső adatbázisokkal vagy hírszerzési adatokkal való összevetésén keresztül. Az egyéneket az összegyűjtött információk alapján egyetlen meglévő rendőrségi adatbázisban sem regisztrálták. A rendőrség úgy dönt, hogy egy magánvállalat által biztosított, fent leírt eszközt használ a személyek biometrikus azonosítás útján történő azonosítására.

Az információ forrása:

- Az érintettek típusai: ☒ minden állampolgár (tanúk) ☒ elítéltek ☒ gyanúsítottak
- A kép forrása: ☒ Nyilvános térben készült vagy előzetes vizsgálat során máshol gyűjtött videofelvételek
- Bűncselekménnyel fennálló kapcsolat: ☒ Nem szükséges
- Az információgyűjtés módja: ☒ távoli
- Kontextus – más alapvető jogokat érint: Igen, nevezetesen: ☒ A gyülekezés szabadsága ☒ A véleménynyilvánítás szabadsága ☒ más alapvető jog

Referencia-adatbázis (amellyel a begyűjtött információkat összehasonlítják):

- Specifikusság: ☒ Az internetről feltöltött általános célú adatbázisok

Algoritmus:

- Az adatkezelés típusa: ☒ azonosítás (egy a többhöz megfeleltetés)

Eredmény

- Hatás ☒ Közvetlen (pl. az érintettet letartóztatják, kihallgatják, diszkriminatív viselkedés)
- Automatizált döntés: ☒ NEM

Jogi elemzés:

- Az érintett előzetes tájékoztatásának típusa: ☒ Nem

6.2. Az alkalmazandó jogi keret

Ha egy magánjogi szervezet olyan szolgáltatást nyújt, amely magában foglalja a személyes adatok olyan feldolgozását, amelynek célját és eszközeit (ebben az esetben képek gyűjtése az internetről egy adatbázis létrehozása céljából) meghatározták, akkor ennek a magánjogi szervezetnek rendelkeznie kell adatkezelési jogalappal. Továbbá a bűnüldöző hatóságnak, amely úgy dönt, hogy ezt a szolgáltatást saját céljaira használja, az adatkezeléshez, amelynek céljait és eszközeit meghatározták, rendelkeznie kell egy jogalappal. Ahhoz, hogy a bűnüldöző hatóság képes legyen biometrikus adatokat kezelni, olyan jogi keretre van szükség, amely meghatározza a célkitűzést, a feldolgozandó személyes adatokat, az adatkezelés céljait, a személyes adatok sértetlenségének és bizalmasságának megőrzését szolgáló eljárásokat, valamint az adatok megsemmisítésére vonatkozó eljárásokat.

E forgatókönyv a személyes adatok tömeges gyűjtését jelenti olyan személyektől, akiknek nincs tudomásuk az adataik gyűjtéséről. Az ilyen adatkezelés csak nagyon kivételes körülmények között lenne jogszerű. Attól függően, hogy hol található az adatbázis, egy ilyen szolgáltatás igénybevétele a személyes adatok és/vagy a személyes adatok különleges kategóriáinak az Európai Unión kívülre történő továbbítását vonhatja maga után (a rendőrség által, pl. a megfigyelési videón szereplő, vagy más módon gyűjtött arcképmás „elküldésével"), ami az ilyen továbbításra vonatkozó különleges feltételek teljesítését követeli meg, lásd LED 39. cikk.

Ebben a forgatókönyvben nincsenek olyan speciális szabályok, amelyek az ilyen típusú adatkezelést megengednék a bűnüldöző hatóság számára.

6.3. Szükségesség és arányosság

A szolgáltatásnak a bűnüldöző hatóság általi igénybevétele azt jelenti, hogy személyes adatokat osztanak meg egy olyan magánszervezettel, amely a személyes adatokat korlátlanul és tömeges módon gyűjtő adatbázist használ. Az összegyűjtött személyes adatok és a bűnüldöző hatóság által kitűzött cél között nem áll fenn kapcsolat. Az adatoknak a bűnüldöző hatóság által a magánjogi szervezettel történő megosztása azt is jelenti, hogy a hatóság nem gyakorol ellenőrzést a magánjogi szervezet által kezelt adatok felett, és az érintettek nagyon nehezen gyakorolhatják jogaikat, mivel nem lesz tudomásuk arról, hogy adataikat ilyen módon kezelik. Ez nagyon szigorú korlátot jelent az olyan helyzetekben, amikor ilyen adatkezelésre akár sor is kerülhet. Kérdéses, hogy bármely célkitűzés megfelelne-e az irányelvben meghatározott követelményeknek, mivel a magánélethez és az adatvédelemhez való jogtól való bármely eltérés, illetve azok korlátozása csak a feltétlenül szükséges esetekben alkalmazható. A súlyos bűncselekmények elleni hatékony küzdelemhez fűződő általános érdek önmagában nem indokolhatja az adatkezelést, ha ilyen nagy mennyiségű adatot gyűjtenek válogatás nélkül. Ez az adatkezelés ezért nem felelne meg a szükségesség és az arányosság követelményeinek.

6.4. Következtetés

Az irányelv 4. és 10. cikkében foglalt követelményeknek megfelelő egyértelmű, pontos és előre látható szabályok hiánya, valamint az arra vonatkozó bizonyítékok hiánya, hogy ez az adatkezelés feltétlenül szükséges a kitűzött célok eléréséhez, arra enged következtetni, hogy ezen alkalmazás használata nem felelne meg a szükségességi és arányossági követelményeknek és aránytalan beavatkozást jelentene az érintetteknek a magánélet tiszteletben tartásához és a személyes adatok védelméhez való, a Charta szerinti jogaiba.