
# Usmernenia 05/2022 o používaní technológie rozpoznávania tváre v oblasti presadzovania práva

## Verzia 2.0

## Prijaté 26. apríla 2023

## História verzií

| | | |
|---|---|---|
| Verzia 1.0 | 12. mája 2022 | Prijatie usmernení na účely verejnej konzultácie |
| Verzia 2.0 | 26. apríla 2023 | Prijatie usmernení po verejnej konzultácii |

# Obsah

# ZHRNUTIE

Čoraz viac orgánov presadzovania práva (ďalej len „OPP“) používa alebo plánuje používať technológiu rozpoznávania tváre (ďalej len „TRT“). Môže sa používať na **autentifikáciu** alebo na **identifikáciu** osoby a môže sa používať pri videozáznamoch (napr. z kamerových systémov) alebo pri fotografiách. Môže sa používať na rôzne účely vrátane hľadania osôb z policajných zoznamov sledovaných osôb alebo na monitorovanie pohybu osôb na verejnom priestranstve.

TRT je založená na spracúvaní **biometrických údajov**, a preto zahŕňa spracúvanie osobitných kategórií osobných údajov. TRT často využíva komponenty **umelej inteligencie** (AI) alebo strojového učenia (machine learning). Hoci sa tým umožňuje rozsiahle spracúvanie údajov, dochádza aj k vzniku rizika diskriminácie a nesprávnych výsledkov. TRT sa môže používať v kontrolovaných situáciách jeden na jedného, ale aj v prípade veľkých davov a vo významných dopravných uzloch.

TRT je **pre orgány presadzovania práva citlivým nástrojom.** OPP sú výkonné orgány a majú suverénne právomoci. TRT má tendenciu zasahovať do základných práv – aj nad rámec práva na ochranu osobných údajov – a je schopná ovplyvňovať našu sociálnu a demokratickú politickú stabilitu.

Pokiaľ ide o ochranu osobných údajov v kontexte presadzovania práva, musia byť splnené **požiadavky smernice o presadzovaní práva** (ďalej len „LED“). Určitý rámec týkajúci sa používania TRT je stanovený v LED, najmä v článku 3 bode 13 tejto smernice (pojem „biometrické údaje“), článku 4 (zásady týkajúce sa spracúvania osobných údajov), článku 8 (zákonnosť spracúvania), článku 10 (spracúvanie osobitných kategórií osobných údajov) a článku 11 LED (automatizované individuálne rozhodovanie).

Uplatňovanie TRT môže mať vplyv aj na niekoľko ďalších základných práv. **Charta základných práv EÚ** (ďalej len „Charta“) je preto pri výklade smernice o presadzovaní práva nevyhnutná, najmä pokiaľ ide o právo na ochranu osobných údajov podľa článku 8 Charty, ale aj právo na súkromie stanovené v článku 7 Charty.

**Legislatívne opatrenia**, ktoré slúžia ako právny základ pre spracúvanie osobných údajov, priamo zasahujú do práv zaručených v článkoch 7 a 8 Charty. Samotné spracúvanie biometrických údajov za akýchkoľvek okolností predstavuje vážny zásah do práv. Platí to bez ohľadu na výsledok, napr. kladný výsledok. Akékoľvek obmedzenie výkonu práv a slobôd musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd.

Právne základy musia byť **dostatočne jasné** na to, aby občanom poskytli primerané informácie o podmienkach a okolnostiach, za ktorých sú orgány oprávnené pristúpiť k akýmkoľvek opatreniam zhromažďovania údajov a tajného sledovania. Len samotnou transpozíciou všeobecného ustanovenia v článku 10 smernice o presadzovaní práva do vnútroštátneho práva by chýbala presnosť a predvídateľnosť.

Predtým, ako vnútroštátny zákonodarca vytvorí nový právny základ pre akúkoľvek formu spracúvania biometrických údajov pomocou rozpoznávania tváre, mal by to **konzultovať** s príslušným dozorným orgánom pre ochranu údajov.

Legislatívne opatrenia musia byť **primerané** na dosiahnutie legitímnych cieľov sledovaných predmetnou právnou úpravou. **Cieľ všeobecného záujmu** – nech už je akokoľvek zásadný – sám osebe neodôvodňuje obmedzenie základného práva. Legislatívne opatrenia by mali **rozlišovať** medzi osobami, na ktoré sa vzťahujú a zameriavať sa na príslušné osoby vzhľadom na cieľ, napr. boj proti konkrétnej závažnej trestnej činnosti. Ak sa opatrenie vzťahuje na všetky osoby všeobecným spôsobom

bez takéhoto rozlišovania, obmedzenia alebo výnimky, prehlbuje sa tým zásah. Zásah sa prehlbuje aj v prípade, ak sa spracúvanie údajov týka významnej časti obyvateľstva.

Údaje sa musia spracúvať spôsobom, ktorý zabezpečuje uplatniteľnosť a účinnosť pravidiel a zásad EÚ na ochranu údajov. Na základe každej situácie sa pri **posúdení nevyhnutnosti a primeranosti** musia identifikovať a zvážiť aj všetky možné dôsledky pre iné základné práva. Ak sa údaje systematicky spracúvajú bez vedomia dotknutých osôb, môže to viesť k **všeobecnému pocitu neustáleho sledovania**. To môže viesť k odstrašujúcim účinkom v súvislosti s niektorými alebo všetkými dotknutými základnými právami, ako je ľudská dôstojnosť podľa článku 1 Charty, sloboda myslenia, svedomia a náboženského vyznania podľa článku 10 Charty, sloboda prejavu podľa článku 11 Charty, ako aj sloboda zhromažďovania a združovania podľa článku 12 Charty.

Spracúvanie osobitných kategórií údajov, ako sú biometrické údaje, možno považovať za „**úplne nevyhnutné**“ (článok 10 LED) len vtedy, ak sa zásah do ochrany osobných údajov a jej obmedzenia obmedzujú na to, čo je absolútne potrebné, t. j. nevyhnutné, a vylučuje akékoľvek spracúvanie všeobecnej alebo systematickej povahy.

Skutočnosť, že dotknutá osoba **preukázateľne sprístupnila** [manifestly made public] fotografiu (článok 10 LED), neznamená, že sa za preukázateľne sprístupnené považujú súvisiace biometrické údaje, ktoré možno získať z fotografie osobitnými technickými prostriedkami. Predvolené nastavenia služby, napr. zverejňovanie vzorov [template], alebo absencia možnosti voľby, napr. zverejňovanie vzorov bez toho, aby používateľ mohol toto nastavenie zmeniť, by sa v žiadnom prípade nemali chápať ako preukázateľne sprístupnené údaje.

V článku 11 LED sa stanovuje rámec pre **automatizované individuálne rozhodovanie**. Používanie TRT zahŕňa používanie osobitných kategórií údajov a môže viesť k profilovaniu v závislosti od spôsobu a účelu uplatňovania TRT. V súlade s právom Únie a článkom 11 ods. 3 LED je každopádne zakázané profilovanie, ktoré vedie k diskriminácii fyzických osôb na základe osobitných kategórií osobných údajov.

Článok 6 LED sa týka potreby **rozlišovať medzi rôznymi kategóriami dotknutých osôb**. Pokiaľ ide o dotknuté osoby, v prípade ktorých neexistuje žiadny dôkaz, z ktorého by mohlo vyplývať, že ich konanie by mohlo hoci len nepriamo alebo vzdialene súvisieť s legitímnym cieľom podľa LED, s najväčšou pravdepodobnosťou neexistuje odôvodnenie zásahu.

**Zásada minimalizácie údajov** [článok 4 ods. 1 písm. e) LED] okrem iného vyžaduje, aby sa akékoľvek videozáznamy, ktoré nie sú relevantné pre účel spracúvania, pred zavedením vždy odstránili alebo anonymizovali (napr. rozmazaním bez možnosti spätného obnovenia údajov).

Prevádzkovateľ musí dôkladne zvážiť, ako (alebo či dokáže) splniť požiadavky na **práva dotknutej osoby** pred začatím akéhokoľvek spracúvania pomocou TRT, keďže TRT často zahŕňa spracúvanie osobitných kategórií osobných údajov bez akejkoľvek zjavnej interakcie s dotknutou osobou.

Účinný výkon práv dotknutej osoby závisí od toho, či prevádzkovateľ plní svoje **informačné povinnosti** (článok 13 LED). Pri posudzovaní toho, či ide o „osobitný prípad“ podľa článku 13 ods. 2 LED, je potrebné zohľadniť niekoľko faktorov vrátane toho, či sa osobné údaje zhromažďujú bez vedomia dotknutej osoby, pretože to by bol jediný spôsob, ako umožniť dotknutým osobám účinne uplatňovať svoje práva. Ak sa rozhodovanie uskutočňuje výlučne na základe TRT, potom je potrebné informovať dotknuté osoby o vlastnostiach automatizovaného rozhodovania.

Pokiaľ ide o **žiadosti o prístup**, ak sú biometrické údaje uložené a spojené s totožnosťou aj prostredníctvom alfanumerických údajov, v súlade so zásadou minimalizácie údajov by to malo

príslušnému orgánu umožniť potvrdiť žiadosť o prístup na základe vyhľadávania podľa týchto alfanumerických údajov a bez toho, aby sa začalo ďalšie spracúvanie biometrických údajov iných osôb (t. j. vyhľadávaním pomocou TRT v databáze).

Riziká pre dotknuté osoby sú obzvlášť závažné, ak sú v policajnej databáze uložené a/alebo iným subjektom poskytované nesprávne údaje. Prevádzkovateľ musí príslušne **opraviť** uložené údaje a systémy TRT (pozri aj odôvodnenie 47 LED).

Právo na **obmedzenie** nadobúda dôležitosť, najmä ak ide o technológiu rozpoznávania tváre [založenú na algoritme (algoritmoch), a teda nikdy nezobrazujúcu definitívny výsledok] v situáciách, keď sa zhromažďuje veľké množstvo údajov a môže dochádzať k identifikácii s rôznou mierou správnosti a kvality.

**Posúdenie vplyvu na ochranu údajov** (ďalej len „DPIA“) pred použitím TRT je povinnou požiadavkou podľa článku 27 LED. Európsky výbor pre ochranu údajov (ďalej len „EDPB“) odporúča zverejniť výsledky takýchto posúdení alebo aspoň hlavné zistenia a závery DPIA ako opatrenie na zvýšenie dôvery a transparentnosti.

Väčšina prípadov zavádzania a používania TRT sa vo svojej podstate vyznačuje vysokým rizikom pre práva a slobody dotknutých osôb. Preto by mal orgán, ktorý zavádza TRT, pred zavedením systému **konzultovať** s príslušným dozorným orgánom.

Vzhľadom na jedinečnú povahu biometrických údajov by mal orgán, ktorý zavádza a/alebo používa TRT, venovať osobitnú pozornosť **bezpečnosti spracúvania**, v súlade s článkom 29 LED. Orgán presadzovania práva by mal predovšetkým zabezpečiť, aby systém spĺňal príslušné normy a mal by zaviesť opatrenia na ochranu biometrických vzorov [biometric template]. Zásady a záruky ochrany údajov musia byť súčasťou technológie už pred začatím spracúvania osobných údajov. Preto aj v prípade, že OPP plánuje uplatňovať a používať TRT od externých poskytovateľov, musí zabezpečiť, napríklad prostredníctvom postupu verejného obstarávania, aby sa zaviedli **len TRT založené na zásadách špecificky navrhnutej a štandardnej ochrany údajov**.

**Logovanie** (pozri článok 25 LED) je dôležitou zárukou overovania zákonnosti spracúvania, a to tak interne (t. j. vlastné monitorovanie zo strany príslušného prevádzkovateľa/sprostredkovateľa), ako aj zo strany externých dozorných orgánov. V súvislosti so systémami rozpoznávania tváre sa logovanie odporúča aj v prípade zmien v referenčnej databáze a pokusov o identifikáciu alebo overenie vrátane používateľa, výsledku a skóre spoľahlivosti. Logovanie je však len jedným zo základných prvkov celkovej **zásady zodpovednosti** (pozri článok 4 ods. 4 LED). Prevádzkovateľ musí byť schopný preukázať súlad spracúvania so základnými zásadami ochrany údajov podľa článku 4 ods. 1 až 3 LED.

EDPB pripomína spoločnú **výzvu** EDPB a EDPS **na zákaz** určitých druhov spracúvania v súvislosti s 1. diaľkovou biometrickou identifikáciou [remote biometric identification] osôb vo verejne prístupných priestoroch, 2. systémami rozpoznávania tváre s podporou umelej inteligencie, ktoré kategorizujú osoby na základe ich biometrických údajov do skupín podľa etnického pôvodu, pohlavia, ako aj podľa politickej alebo sexuálnej orientácie alebo iných dôvodov na diskrimináciu, 3. používaním rozpoznávania tváre alebo podobných technológií na odvodenie emócií fyzickej osoby a 4. spracúvanie osobných údajov v kontexte presadzovania práva, ktoré by sa opieralo o databázu naplnenú zhromažďovaním osobných údajov v masovom rozsahu a nediferencovaným spôsobom, napr. extrahovaním (scraping) fotografií a obrázkov tváre dostupných online.

Ústrednou zárukou dotknutých základných práv je **účinný dohľad** zo strany príslušných dozorných orgánov pre ochranu údajov. Členské štáty preto musia zabezpečiť, aby zdroje dozorných orgánov boli primerané a dostatočné na to, aby mohli plniť svoj mandát.

**Tieto usmernenia** sú určené zákonodarcom na úrovni EÚ a na vnútroštátnej úrovni, ako aj OPP a ich príslušníkom pri zavádzaní a používaní systémov TRT. Pre jednotlivcov sú určené len pokiaľ sa o nich zaujímajú všeobecne, resp. ako dotknuté osoby, najmä pokiaľ ide o práva dotknutých osôb.

**Cieľom týchto usmernení** je informovať o určitých vlastnostiach TRT a o uplatniteľnom právnom rámci v kontexte presadzovania práva (najmä LED).

- Okrem toho poskytujú **nástroj na podporu prvej klasifikácie citlivosti daného prípadu použitia** (Príloha I).
- Obsahujú aj **praktické usmernenia pre OPP, ktoré majú záujem obstarať a prevádzkovať systém TRT** (príloha II).
- V usmerneniach sa okrem toho uvádza niekoľko typických **prípadov použitia a zoznam mnohých relevantných aspektov**, najmä pokiaľ ide o test nevyhnutnosti a primeranosti (príloha III).

# 1 ÚVOD

1. Technológia rozpoznávania tváre (TRT) sa môže použiť na automatické rozpoznávanie osôb na základe ich tváre. TRT je často založená na umelej inteligencii, ako sú napríklad technológie strojového učenia. Aplikácie TRT sa čoraz častejšie testujú a používajú v rôznych oblastiach, od individuálneho použitia až po využívanie v súkromných organizáciách a verejnej správe. Aj orgány presadzovania práva očakávajú výhody z využívania TRT. Sľubuje riešenia relatívne nových výziev, ako sú vyšetrovania zahŕňajúce veľké množstvo získaných dôkazov, ale aj známych problémov, najmä pokiaľ ide o nedostatočné personálne obsadenie pri vykonávaní úloh pozorovania a pátrania.

2. Veľká časť zvýšeného záujmu o TRT vyplýva z efektívnosti a rozšíriteľnosti TRT. S tým sa však spájajú aj nevýhody, ktoré sú tejto technológii a jej uplatňovaniu vlastné – a to aj vo veľkom rozsahu. Je síce možné stlačením tlačidla analyzovať tisíce súborov osobných údajov, no aj tie najmenšie účinky algoritmickej diskriminácie alebo nesprávnej identifikácie môžu viesť k vážnym následkom pre správanie a každodenný život vysokého počtu osôb. Už len samotný rozsah spracúvania osobných údajov, a najmä biometrických údajov, je ďalším kľúčovým prvkom TRT, keďže spracúvanie osobných údajov predstavuje zásah do základného práva na ochranu osobných údajov podľa článku 8 Charty základných práv Európskej únie (ďalej len „Charta“).

3. Uplatňovanie TRT zo strany OPP bude mať - a do určitej miery už má - významné dôsledky pre jednotlivcov a skupiny ľudí vrátane menšín. Tieto dôsledky budú mať značný vplyv aj na spôsob nášho spolužitia a na našu sociálnu a demokratickú politickú stabilitu, ktorá oceňuje a kladie veľký dôraz na pluralizmus a politickú opozíciu. Právo na ochranu osobných údajov je často kľúčovým predpokladom na zaručenie ďalších základných práv. Pri uplatňovaní TRT existuje značná tendencia zasahovať do základných práv nad rámec práva na ochranu osobných údajov.

4. EDPB preto považuje za dôležité prispieť k prebiehajúcej integrácii TRT v oblasti presadzovania práva, na ktorú sa vzťahuje smernica o presadzovaní práva[1], resp. vnútroštátne právne predpisy, ktorými sa transponuje, a poskytnúť tieto usmernenia. Cieľom týchto usmernení je poskytnúť relevantné informácie zákonodarcom na úrovni EÚ a na vnútroštátnej úrovni, ako aj orgánom presadzovania práva a ich príslušníkom pri zavádzaní a používaní systémov TRT. Rozsah pôsobnosti usmernení je obmedzený na TRT. Aj iné formy spracúvania osobných údajov na základe biometrických údajov orgánmi presadzovania práva, najmä ak sa spracúvajú na diaľku, však môžu predstavovať podobné alebo dodatočné riziká pre jednotlivcov, skupiny a spoločnosť. Vzhľadom na konkrétne okolnosti môžu niektoré aspekty týchto usmernení slúžiť ako užitočný zdroj aj v takýchto prípadoch. A napokon, dôležité informácie tu môžu nájsť aj jednotlivci, ktorí sa o tému zaujímajú všeobecne alebo ako dotknuté osoby, najmä pokiaľ ide o práva dotknutých osôb.

5. Usmernenia pozostávajú z hlavného dokumentu a troch príloh. Tento hlavný dokument predstavuje technológiu a uplatniteľný právny rámec. Vzor nápomocný pri identifikácii niektorých z hlavných aspektov klasifikácie závažnosti zásahu do základných práv v danej oblasti uplatňovania možno nájsť v prílohe I. OPP, ktoré majú záujem obstarať a prevádzkovať systém TRT, môžu nájsť praktické usmernenia v prílohe II. V závislosti od oblasti uplatňovania TRT by mohli byť relevantné rôzne aspekty. Súbor hypotetických scenárov a relevantných aspektov možno nájsť v prílohe III.

# 2 TECHNOLÓGIA

## 2.1 Jedna biometrická technológia, dve rôzne funkcie

6. Rozpoznávanie tváre je pravdepodobnostná technológia, ktorá dokáže automaticky rozpoznať osoby podľa ich tváre, umožňujúc tak ich autentifikáciu alebo identifikáciu.

7. TRT patrí do širšej kategórie biometrickej technológie. K biometrii patria všetky automatizované procesy, ktoré sa používajú na rozpoznanie jednotlivca na základe kvantifikácie fyzických, fyziologických alebo behaviorálnych charakteristík (odtlačky prstov, štruktúra dúhovky, hlas, chôdza, štruktúra ciev, atď.). Tieto charakteristiky sú definované ako „biometrické údaje“, pretože umožňujú alebo potvrdzujú jedinečnú identifikáciu danej osoby.

8. Platí to pri tvárach ľudí alebo, presnejšie, pri ich technickom spracovaní pomocou zariadení na rozpoznávanie tváre: nasnímaním snímky tváre [image of a face] (fotografie alebo videa), ktorý sa nazýva biometrická „vzorka“ [biometric sample], je možné získať digitálnu reprezentáciu špecifických charakteristík tejto tváre (nazýva sa „vzor“).

9. Biometrický vzor je digitálna reprezentácia jedinečných znakov, ktoré boli extrahované z biometrickej vzorky a môžu byť uložené v biometrickej databáze[2]. Tento vzor má byť jedinečný a špecifický pre každú osobu a v zásade sa časom nemení[3]. Vo fáze rozpoznávania zariadenie porovnáva tento vzor s inými vzormi, ktoré boli predtým vytvorené alebo vypočítané priamo z biometrických vzoriek, ako sú tváre nájdené na snímke [image], fotografii alebo videu. „Rozpoznávanie tváre“ je preto dvojstupňový

[1] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV.

[2] Usmernenia o rozpoznávaní tváre, Poradný výbor dohovoru č. 108 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, Rada Európy, jún 2021.

[3] Môže to závisieť od druhu biometrie a veku dotknutej osoby.

proces: získanie snímky tváre [facial image] a jeho transformácia na vzor, po ktorom nasleduje rozpoznanie tejto tváre porovnaním príslušného vzoru s jednou alebo viacerými inými vzormi.

10. Rovnako ako akýkoľvek biometrický proces, aj rozpoznávanie tváre môže plniť dve odlišné funkcie:

- **autentifikácia** osoby, ktorej cieľom je overiť, či je osoba tou osobou, za ktorú sa vydáva. Pri autentifikácii systém porovná vopred zaznamenaný biometrický vzor alebo vzorku (napr. uložený na čipovej karte alebo biometrickom pase) s konkrétnou tvárou, napríklad tvárou osoby, ktorá sa dostaví na kontrolné stanovisko, aby sa overilo, či ide o jednu a tú istú osobu. Táto funkcia sa preto spolieha na porovnanie dvoch vzorov. Tento postup sa nazýva aj **overovanie** jedna k jednej.

- **identifikácia** osoby, ktorej cieľom je nájsť konkrétnu osobu v skupine osôb, v rámci určitej oblasti, snímky alebo databázy. V tomto prípade musí systém spracovať každú zaznamenanú tvár, vygenerovať biometrický vzor a potom skontrolovať, či sa zhoduje s osobou, ktorú systém pozná. Táto funkcia teda vychádza z porovnania jedného vzoru s databázou vzorov alebo vzoriek (východiskový vzor) [baseline]. Tento postup sa nazýva aj identifikácia porovnaním jedného údaja s viacerými údajmi. Môže napríklad prepojiť záznam o mene osoby (priezvisko, meno) s tvárou, ak sa porovnanie vykonáva s databázou fotografií spojených s priezviskami a menami. Môže zahŕňať aj sledovanie osoby v dave bez toho, aby nevyhnutne došlo k prepojeniu s občianskou totožnosťou osoby.

11. V oboch prípadoch sú použité techniky rozpoznávania tváre založené na odhadovanej zhode medzi vzormi: porovnávaným vzorom a východiskovým vzorom (vzormi). Z tohto hľadiska sú tieto techniky pravdepodobnostné: porovnaním sa odvodzuje vyššia alebo nižšia pravdepodobnosť, že osoba je skutočne osobou, ktorá sa má autentifikovať alebo identifikovať; ak táto pravdepodobnosť prekročí určitú prahovú hodnotu, ktorú v systéme definoval používateľ alebo vývojár systému, systém bude predpokladať, že existuje zhoda.

12. Hoci sú obe funkcie – autentifikácia a identifikácia – odlišné, obe sa týkajú spracúvania biometrických údajov súvisiacich s identifikovanou alebo identifikovateľnou fyzickou osobou, a preto predstavujú spracúvanie osobných údajov a konkrétnejšie spracúvanie osobitných kategórií osobných údajov.

13. Rozpoznávanie tváre je súčasťou širšieho spektra techník spracovania videozáznamov. Niektoré videokamery dokážu snímať ľudí vo vymedzenej oblasti, najmä ich tváre, nedajú sa však použiť na automatické rozpoznávanie osôb. To isté platí aj pre obyčajné fotografovanie: fotoaparát nie je systém na rozpoznávanie tváre, pretože fotografie ľudí sa musia spracovať špecifickým spôsobom, aby sa z nich dali získať biometrické údaje.

14. Samotná detekcia tvárí takzvanými "inteligentnými" fotoaparátmi tiež nemusí nevyhnutne predstavovať systém rozpoznávania tvárí. Hoci digitálne techniky na zisťovanie abnormálneho správania alebo násilných udalostí alebo na rozpoznávanie emócií tváre či dokonca siluety vyvolávajú zásadné otázky z hľadiska etiky a účinnosti, nemožno ich považovať za biometrické systémy spracúvajúce osobitné kategórie osobných údajov za predpokladu, že ich cieľom nie je jednoznačná identifikácia osoby a že príslušné spracúvanie osobných údajov nezahŕňa iné osobitné kategórie osobných údajov. Tieto príklady nie sú úplne mimo oblasti rozpoznávania tváre a tak či tak podliehajú pravidlám ochrany osobných údajov.[4] Okrem toho sa tento typ systému detekcie môže používať v

[4] Článok 10 LED (alebo článok 9 všeobecného nariadenia o ochrane údajov) sa však vzťahuje na systémy, ktoré sa používajú na kategorizáciu osôb na základe ich biometrických údajov do skupín podľa etnického pôvodu, ako aj politickej alebo sexuálnej orientácie alebo iných osobitných kategórií osobných údajov.

spojení s inými systémami zameranými na identifikáciu osoby, a preto sa môže považovať za technológiu rozpoznávania tváre.

15. Na rozdiel napríklad od systémov na zachytávanie a spracovanie videa, ktoré si vyžadujú inštaláciu fyzických zariadení, rozpoznávanie tváre je softvérová funkcia, ktorú možno zaviesť v rámci existujúcich systémov (kamery, databázy snímok atď.). Takáto funkcia môže byť preto spojená alebo prepojená s mnohými systémami a kombinovaná s inými funkciami. Takáto integrácia do už existujúcej infraštruktúry si vyžaduje osobitnú pozornosť, pretože sa spája s rizikami, ktoré sú tejto technológii vlastné, vzhľadom na skutočnosť, že technológia rozpoznávania tváre by mohla byť uplatňovaná jednoducho a mohla by byť ľahko ukrytá[5].

## 2.2 Široké spektrum účelov a uplatnení

16. Nad rámec rozsahu pôsobnosti týchto usmernení a mimo rozsahu pôsobnosti LED sa rozpoznávanie tváre môže použiť na dosahovanie širokej škály cieľov, a to tak na komerčné použitie, ako aj na riešenie otázok verejnej bezpečnosti alebo presadzovania práva. Môže sa uplatňovať v mnohých rôznych kontextoch: v osobnom vzťahu medzi používateľom a službou (prístup k aplikácii), na prístup na konkrétne miesto (fyzické filtrovanie) alebo bez akéhokoľvek konkrétneho obmedzenia vo verejnom priestore (rozpoznávanie tváre v reálnom čase). Môže sa vzťahovať na akýkoľvek druh dotknutej osoby: zákazníka služby, zamestnanca, obyčajnú prizerajúcu sa osobu, hľadanú osobu alebo osobu zapletenú do súdneho alebo správneho konania atď. Niektoré spôsoby použitia sú už bežné a rozšírené, iné sú v súčasnosti v experimentálnej alebo špekulatívnej fáze. Hoci sa tieto usmernenia nebudú zaoberať všetkými takýmito použitiami a uplatneniami, EDPB pripomína, že sa môžu zavádzať len vtedy, ak sú v súlade s uplatniteľným právnym rámcom, a najmä so všeobecným nariadením o ochrane údajov a príslušnými vnútroštátnymi právnymi predpismi.[6] Aj v kontexte LED sa okrem funkcií autentifikácie alebo identifikácie môžu údaje spracúvané pomocou technológie rozpoznávania tváre ďalej spracúvať aj na iné účely, ako je kategorizácia.

17. Konkrétnejšie, o spektre potenciálnych použití by sa mohlo uvažovať v závislosti od stupňa kontroly, ktorú majú ľudia nad svojimi osobnými údajmi, od účinných prostriedkov, ktoré majú k dispozícii na vykonávanie takejto kontroly, a ich práva dať podnet na spustenie a používanie tejto technológie, dôsledkov pre nich (v prípade rozpoznania alebo nerozpoznania) a rozsahu vykonaného spracúvania. Rozpoznávanie tváre na základe vzoru uloženého na osobnom zariadení (čipová karta, smartfón atď.), ktoré patrí tejto osobe a ktoré sa používa na autentifikáciu a výlučne na osobné použitie prostredníctvom vyhradeného rozhrania, nepredstavuje rovnaké riziká ako napríklad používanie na účely identifikácie v nekontrolovanom prostredí bez aktívnej účasti dotknutých osôb, kde sa vzor každej osoby vstupujúcej do monitorovanej oblasti porovnáva so vzormi širokého záberu obyvateľstva uloženými v databáze. Medzi týmito dvoma extrémami existuje veľmi pestré spektrum spôsobov použitia a súvisiacich otázok týkajúcich sa ochrany osobných údajov.

18. V záujme ďalšej ilustrácie kontextu, v ktorom sa v súčasnosti diskutuje o technológiách na rozpoznávanie tváre alebo sa tieto technológie v rámci neho zavádzajú, či už na účely autentifikácie alebo identifikácie, EDPB považuje za relevantné uviesť viacero príkladov. Ďalej uvedené príklady sú výlučne ilustračné a nemali by sa považovať za žiadne predbežné posúdenie ich súladu s *acquis* EÚ v oblasti ochrany údajov.

*Príklady autentifikácie na základe rozpoznávania tváre*

[5] Napríklad v kamerách nosených na tele, ktoré sa v praxi používajú čoraz častejšie.

[6] Ďalšie informácie nájdete aj v usmerneniach EDPB 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení, ktoré boli prijaté 29. januára 2020.

19. Autentifikácia môže byť navrhnutá tak, aby používatelia mali nad ňou plnú kontrolu, napríklad s cieľom umožniť prístup k službám alebo aplikáciám výlučne v domácom prostredí. Majitelia smartfónov ju preto v rozsiahlej miere používajú na odblokovanie svojho zariadenia namiesto autentifikácie pomocou hesla.

20. Autentifikácia na základe rozpoznávania tváre sa môže použiť aj na kontrolu totožnosti niekoho, kto má záujem využívať verejné alebo súkromné služby tretích strán. Takéto procesy tak ponúkajú spôsob, ako vytvoriť digitálnu identitu pomocou mobilnej aplikácie (smartfón, tablet atď.), ktorá sa potom môže použiť na prístup k online administratívnym službám.

21. Okrem toho môže byť autentifikácia na základe rozpoznávania tváre zameraná na kontrolu fyzického prístupu na jedno alebo viacero vopred určených miest, ako sú napríklad vchody do budov alebo konkrétne priechody. Táto funkcia sa napríklad používa pri určitom spracúvaní na účely prekračovania hraníc, kde sa tvár osoby na zariadení na kontrolnom stanovisku porovnáva s tvárou uloženou v jej doklade totožnosti (pas alebo zabezpečené povolenie na pobyt).

*Príklady identifikácie na základe rozpoznávania tváre*

22. Identifikácia sa môže vykonávať mnohými, ešte oveľa rozmanitejšími spôsobmi. Okrem iného k nim patria nižšie uvedené spôsoby použitia, ktoré sú v súčasnosti v EÚ pozorované, experimentuje sa s nimi alebo sú plánované.

- vyhľadávanie totožnosti neidentifikovanej osoby (obete, podozrivého atď.) v databáze fotografií;
- monitorovanie pohybu osoby na verejnom priestranstve. Tvár osoby sa porovnáva s biometrickými vzormi osôb, ktoré cestujú alebo cestovali v monitorovanej oblasti, napríklad pri zanechaní batožiny alebo po spáchaní trestného činu;
- rekonštrukcia cesty osoby a jej následných interakcií s inými osobami pomocou neskoršieho porovnania tých istých prvkov v snahe identifikovať napríklad kontakty;
- diaľková biometrická identifikácia hľadaných osôb na verejných priestranstvách. Všetky tváre zachytené naživo kamerami sa v reálnom čase porovnávajú s databázou bezpečnostných zložiek;
- automatické rozpoznávanie ľudí na snímke s cieľom identifikovať napríklad ich vzťahy na sociálnej sieti, ktorá ho využíva. Snímka sa porovnáva so vzormi všetkých osôb v rámci siete, ktoré súhlasili s touto funkciou, aby mohla byť navrhnutá menovitá identifikácia týchto vzťahov;
- prístup k službám, pričom niektoré bankomaty rozpoznávajú svojich zákazníkov porovnaním tváre zachytenej kamerou s databázou snímok tvárí, ktorú má banka k dispozícii;
- sledovanie trasy cestujúceho v určitej fáze cesty. V reálnom čase vypočítaný vzor každej osoby, ktorá sa prihlási v bodoch umiestnených v určitých fázach cesty (miesta na odovzdanie batožiny, nástupné vchody atď.), sa porovnáva so vzormi osôb, ktoré boli v systéme zaregistrované predtým.

23. Okrem používania TRT v oblasti presadzovania práva si široké spektrum pozorovaných uplatnení určite vyžaduje komplexnú diskusiu a politický prístup s cieľom zabezpečiť konzistentnosť a súlad s *acquis* EÚ v oblasti ochrany údajov.

## 2.3 Spoľahlivosť, správnosť a riziká pre dotknuté osoby

24. Tak ako každá technológia, aj rozpoznávanie tváre môže čeliť výzvam pri implementácii, najmä pokiaľ ide o jej spoľahlivosť a účinnosť z hľadiska autentifikácie alebo identifikácie, ako aj celkovú otázku kvality a správnosti „zdrojových“ údajov a výsledku spracovania technológie rozpoznávania tváre.

25. Takéto technologické výzvy so sebou prinášajú osobitné riziká pre dotknuté osoby, ktoré sú o to významnejšie alebo závažnejšie v oblasti presadzovania práva, a to vzhľadom na možné účinky na dotknuté osoby, či už právne, alebo iné, ktoré ich podobným spôsobom významne ovplyvňujú. V tejto súvislosti môže byť užitočné zdôrazniť, že následné používanie TRT nie je ako také bezpečnejšie, keďže jednotlivcov možno sledovať v priebehu času a na rôznych miestach. Preto aj následné použitie má svoje špecifické riziká, ktoré sa musia posudzovať individuálne.[7]

26. Ako uviedla Agentúra EÚ pre základné práva vo svojej správe z roku 2019, „určenie potrebnej miery presnosti softvéru na rozpoznávanie tváre je náročné: existuje mnoho rôznych spôsobov hodnotenia a posúdenia správnosti, a to aj v závislosti od úlohy, účelu a kontextu jeho používania. Pri použití technológie na miestach, ktoré navštevujú milióny ľudí, ako sú vlakové stanice alebo letiská, relatívne malý podiel chýb (napr. 0,01 %)[8] stále znamená, že stovky ľudí sú nesprávne označené. Okrem toho pri niektorých kategóriách osôb môže existovať vyššia pravdepodobnosť nesprávnej zhody ako pri iných, ako je opísané v časti 3. Existujú rôzne spôsoby výpočtu a interpretácie chybovosti, preto sa vyžaduje opatrnosť. Okrem toho, pokiaľ ide o správnosť a chybovosť, sú dôležité otázky týkajúce sa toho, ako ľahko možno systém oklamať napríklad falošnými snímkami tváre (tzv. „spoofing“), a to najmä na účely presadzovania práva."[9]

27. V tejto súvislosti EDPB považuje za dôležité pripomenúť, že TRT, bez ohľadu na to, či sa používa na účely autentifikácie alebo identifikácie, neposkytuje definitívny výsledok, ale vychádza z pravdepodobnosti, že dve tváre alebo snímky tváre zodpovedajú tej istej osobe.[10] Tento výsledok sa ďalej zhoršuje, keď je kvalita biometrickej vzorky, ktorá je podkladom pre rozpoznávanie tváre, nízka. Faktormi nízkej kvality môžu byť rozmazanosť vstupných snímok, nízke rozlíšenie kamery, pohyb a slabé osvetlenie. Ďalšími aspektmi s významným vplyvom na výsledky sú prevalencia a spoofing, napr. keď sa zločinci snažia buď vyhnúť pohybu v blízkosti kamier, alebo oklamať TRT. Viaceré štúdie tiež zdôraznili, že takéto štatistické výsledky algoritmického spracúvania môžu takisto podliehať skresleniu, najmä v dôsledku kvality zdrojových údajov, ako aj z tréningových databáz [training databases] alebo iných faktorov, ako je výber miesta použitia. Okrem toho by sa mal zdôrazniť vplyv technológie rozpoznávania tváre na iné základné práva, ako je rešpektovanie súkromného a rodinného života, sloboda prejavu a právo na informácie, sloboda zhromažďovania a združovania atď.

28. Preto je nevyhnutné, aby sa spoľahlivosť a presnosť technológie rozpoznávania tváre zohľadňovali ako kritériá pri posudzovaní súladu s kľúčovými zásadami ochrany údajov podľa článku 4 LED, a najmä pokiaľ ide o spravodlivosť a správnosť.

29. EDPB zdôrazňuje, že pre vysokokvalitné algoritmy sú nevyhnutné vysokokvalitné údaje, zároveň však zdôrazňuje, že je potrebné, aby prevádzkovatelia v rámci svojej povinnosti niesť zodpovednosť vykonávali pravidelné a systematické hodnotenie algoritmického spracúvania s cieľom zabezpečiť najmä správnosť, spravodlivosť a spoľahlivosť výsledku takéhoto spracúvania osobných údajov. Osobné údaje používané na účely hodnotenia, tréningu a ďalšieho vývoja systémov TRT sa môžu spracúvať len na základe dostatočného právneho základu a v súlade so spoločnými zásadami ochrany údajov.

[7] Pozri príklady uvedené v prílohe III.

[8] Táto miera správnosti vyplýva z citovanej správy a odráža oveľa lepšiu mieru, než je súčasná výkonnosť algoritmov pri uplatňovaní TRT.

[9] Technológia rozpoznávania tváre: úvahy o základných právach v kontexte presadzovania práva, Agentúra EÚ pre základné práva, 21. novembra 2019.

[10] Táto pravdepodobnosť sa označuje ako „skóre spoľahlivosti“.

# 3 UPLATNITEĽNÝ PRÁVNY RÁMEC

30. Používanie technológií rozpoznávania tváre je neoddeliteľne spojené so spracúvaním osobných údajov vrátane osobitných kategórií údajov. Okrem toho má priamy alebo nepriamy vplyv na viaceré základné práva zakotvené v Charte základných práv Európskej únie. Toto je obzvlášť dôležité v oblasti presadzovania práva a trestného súdnictva. Každé použitie technológií rozpoznávania tváre by sa preto malo vykonávať v prísnom súlade s uplatniteľným právnym rámcom.

31. Nasledujúce informácie sa majú zvážiť pri posudzovaní budúcich legislatívnych a administratívnych opatrení, ako aj pri uplatňovaní existujúcich právnych predpisov v jednotlivých prípadoch, ktoré sa týkajú TRT. Relevantnosť príslušných požiadaviek sa líši v závislosti od konkrétnych okolností. Keďže nie je možné predvídať všetky budúce okolnosti, považuje sa len ako poskytnutie podpory a nemá sa chápať tak, že ide o vyčerpávajúci zoznam.

## 3.1 Všeobecný právny rámec – Charta základných práv EÚ a Európsky dohovor o ľudských právach (EDĽP)

### 3.1.1 Uplatniteľnosť Charty

32. Charta základných práv EÚ (ďalej len „Charta“) sa vzťahuje na inštitúcie, orgány, úrady a agentúry Únie a členským štátom pri vykonávaní práva Únie.

33. Pri regulácii spracúvania biometrických údajov na účely presadzovania práva podľa článku 1 ods. 1 LED nevyhnutne vzniká otázka dodržiavania základných práv, najmä rešpektovania súkromného života a komunikácie podľa článku 7 Charty a práva na ochranu osobných údajov podľa článku 8 Charty.

34. Zhromažďovanie a analýza videozáznamov fyzických osôb vrátane ich tvárí znamená spracúvanie osobných údajov. Pri technickom spracovaní snímok sa spracúvanie vzťahuje aj na biometrické údaje. Technické spracúvanie údajov týkajúcich sa tváre fyzickej osoby v súvislosti s časom a miestom umožňuje vyvodiť závery týkajúce sa súkromného života príslušných osôb. Tieto závery sa môžu týkať rasového alebo etnického pôvodu, zdravia, náboženstva, každodenných návykov, trvalých alebo dočasných miest pobytu, každodenného alebo iného pohybu, vykonávaných činností, sociálnych vzťahov týchto osôb a sociálneho prostredia, v ktorom sa pohybujú. Z veľkého rozsahu informácií, ktoré môžu byť odhalené uplatnením TRT, jasne vyplýva možný vplyv na právo na ochranu osobných údajov stanovené v článku 8 Charty, ale aj na právo na súkromie stanovené v článku 7 Charty.

35. Za týchto okolností takisto nie je nepredstaviteľné, že získavanie, analýza a ďalšie spracúvanie predmetných biometrických údajov (o tvári) môže mať vplyv na ľudské vnímanie slobody konať, aj keď by bolo konanie úplne v medziach slobodnej a otvorenej spoločnosti. Môže mať takisto vážne dôsledky na výkon základných práv ľudí, ako je ich právo na slobodu myslenia, svedomia a náboženstva, slobodu vyjadrenia a pokojného zhromažďovania a združovania podľa článkov 1, 10, 11 a 12 Charty. Takéto spracúvanie zahŕňa aj iné riziká, ako je riziko zneužitia osobných informácií zhromaždených príslušnými orgánmi v dôsledku nezákonného prístupu k osobným údajom a ich použitia, narušenia bezpečnosti atď. Riziká často závisia od spracúvania a jeho okolností, ako je riziko nezákonného prístupu a použitia príslušníkmi polície alebo inými neoprávnenými stranami. Niektoré riziká sú však jednoducho neoddeliteľnou súčasťou jedinečnej povahy biometrických údajov. Na rozdiel od adresy alebo telefónneho čísla, nie je možné, aby dotknutá osoba zmenila svoje jedinečné charakteristiky ako je tvár alebo dúhovka. V prípade neoprávneného prístupu alebo náhodného uverejnenia biometrických údajov by to viedlo k znehodnoteniu týchto údajov pri ich používaní ako hesiel alebo kryptografických

kľúčov, alebo by sa tieto údaje mohli použiť na ďalšie, nepovolené činnosti sledovania na úkor dotknutej osoby.

### 3.1.2 Zásah do práv stanovených v Charte

36. Samotné spracúvanie biometrických údajov za akýchkoľvek okolností predstavuje vážny zásah do práv. Platí to bez ohľadu na výsledok, napr. kladný výsledok. Spracúvanie predstavuje zásah aj vtedy, ak sa biometrický vzor vymaže okamžite po porovnaní s policajnou databázou bez kladného výsledku.

37. Zásah do základných práv dotknutých osôb môže vyplývať z právneho aktu, ktorého cieľom alebo dôsledkom je obmedzenie príslušného základného práva[11]. Môže vyplývať aj z právneho úkonu orgánu verejnej moci s rovnakým účelom alebo účinkom, alebo dokonca súkromného subjektu, ktorý je zo zákona poverený výkonom verejnej moci a verejných právomocí.

38. Legislatívne opatrenia, ktoré slúžia ako právny základ pre spracúvanie osobných údajov, priamo zasahujú do práv zaručených v článkoch 7 a 8 Charty[12].

39. Používanie biometrických údajov a najmä TRT má v mnohých prípadoch vplyv aj na právo na ľudskú dôstojnosť zaručené v článku 1 Charty. Ľudská dôstojnosť si vyžaduje, aby sa s ľuďmi nezaobchádzalo len ako s objektmi. TRT vypočítava existenčné a veľmi osobné charakteristiky, črty tváre, do strojovo čitateľnej podoby s cieľom použiť ich ako poznávaciu značku alebo preukaz totožnosti človeka, čím tvár objektivizuje.

40. Takéto spracúvanie môže zasahovať aj do iných základných práv, ako sú práva podľa článkov 10, 11 a 12 Charty, pokiaľ sú odstrašujúce účinky buď zamýšľané, alebo vyplývajú z príslušného kamerového dohľadu orgánov presadzovania práva.

41. Okrem toho by sa mali starostlivo zvážiť aj potenciálne riziká vyplývajúce z používania technológií rozpoznávania tváre orgánmi presadzovania práva, pokiaľ ide o právo na spravodlivý proces a prezumpciu neviny podľa článkov 47 a 48 Charty. Výsledok uplatňovania TRT, napr. zhoda, môže viesť nielen k tomu, že osoba bude podrobená ďalším policajným opatreniam, ale môže byť aj rozhodujúcim dôkazom v súdnom konaní. Nedostatky TRT, ako je možné skreslenie, diskriminácia alebo nesprávna identifikácia („falošne pozitívny výsledok“), môžu mať preto vážne dôsledky aj pre trestné konanie. Okrem toho pri posudzovaní dôkazov môže byť uprednostnený výsledok uplatnenia TRT, aj napriek existencii protichodných dôkazov („nadmerné dôverovanie automatizácii“) [automation bias].

### 3.1.3 Odôvodnenie zásahu

42. Podľa článku 52 ods. 1 Charty akékoľvek obmedzenie výkonu základných práv a slobôd musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Európskou úniou, alebo ak je to potrebné na ochranu práv a slobôd iných.

#### *3.1.3.1 Ustanovené zákonom*

43. V článku 52 ods. 1 Charty sa stanovuje požiadavka osobitného právneho základu. Tento právny základ musí byť dostatočne jasný na to, aby občanom poskytol primerané informácie o podmienkach a okolnostiach, za ktorých sú orgány oprávnené pristúpiť k akýmkoľvek opatreniam zhromažďovania

[11] Rozsudok SDEÚ vo veci C-219/91 – Ter Voort, RoC 1992 I-05485, bod 36f; rozsudok SDEÚ vo veci C-200/96 – Metronome, RoC 1998 I-1953, bod 28.
[12] Rozsudok SDEÚ vo veci C-594/12, bod 36; rozsudok SDEÚ vo veci C-291/12, bod 23 a nasledujúce.

údajov a tajného sledovania[13]. Musí dostatočne jasne uvádzať rozsah a spôsob výkonu príslušnej diskrečnej právomoci zverenej orgánom verejnej moci, aby sa jednotlivcom zabezpečila minimálna miera ochrany, na ktorú majú v demokratickej spoločnosti právo podľa zásad právneho štátu[14]. Zákonnosť si okrem toho vyžaduje primerané záruky, aby sa zabezpečilo najmä dodržiavanie práva jednotlivca podľa článku 8 Charty. Tieto zásady sa vzťahujú aj na spracúvanie osobných údajov na účely hodnotenia, tréningu a ďalšieho vývoja systémov TRT.

44. Vzhľadom na to, že biometrické údaje spracúvané na účely jedinečnej identifikácie fyzickej osoby predstavujú osobitné kategórie údajov uvedené v článku 10 LED, rôzne aplikácie na základe TRT by si vo väčšine prípadov vyžadovali osobitný právny predpis, v ktorom by sa presne opísala aplikácia a podmienky jej použitia. To zahŕňa najmä druhy trestných činov a prípadne primeranú hranicu závažnosti týchto trestných činov s cieľom okrem iného účinne vylúčiť drobnú trestnú činnosť.[15]

#### *3.1.3.2 Podstata základného práva na súkromie a na ochranu osobných údajov stanovených v článkoch 7 a 8 Charty*

45. Obmedzenia základných práv, ktoré sú bezprostredné v každej situácii, musia stále zabezpečovať rešpektovanie podstaty konkrétneho práva. Táto podstata odkazuje na samotné jadro príslušného základného práva[16]. Musí sa rešpektovať aj ľudská dôstojnosť, a to aj v prípadoch, keď je právo obmedzené[17].

46. Náznaky možného porušenia nedotknuteľnej podstaty sú tieto:

- Ustanovenie, ktoré stanovuje obmedzenia bez ohľadu na individuálne správanie osoby alebo na výnimočné okolnosti[18].
- Obrátiť sa na súd nie je možné, alebo sa tomu bráni[19].
- Pred prísnym obmedzením sa neberú do úvahy okolnosti dotknutého jednotlivca[20].
- So zreteľom na práva podľa článkov 7 a 8 Charty: Okrem všeobecného zhromažďovania metaúdajov o komunikácii by nadobudnutím vedomostí o obsahu elektronickej komunikácie mohlo dôjsť k porušeniu podstaty týchto práv[21].
- So zreteľom na práva podľa článkov 7, 8 a 11 Charty: Právne predpisy, v ktorých sa vyžaduje, aby poskytovatelia prístupu k online verejným komunikačným službám a poskytovatelia hostingových služieb vo všeobecnosti a bez rozdielu uchovávali okrem iného osobné údaje týkajúce sa týchto služieb[22].
- S odkazom na práva podľa článku 8 Charty: Chýbajúce základné zásady ochrany a bezpečnosti údajov by mohli takisto porušovať podstatu práva[23].

[13] ESĽP, Shimovolos/Rusko, bod 68; Vukota-Bojić/Švajčiarsko.
[14] ESĽP, Piechowicz/Poľsko, bod 212.
[15] Pozri napr. rozsudky SDEÚ vo veciach C-817/19 Ligue des droits humains, bod 151 f, vo veci C-207/16 Ministerio Fiscal, bod 56.
[16] Rozsudok SDEÚ vo veci C-279/09, RoC 2010 I-13849, bod 60.
[17] Vysvetlenia k Charte základných práv, hlava I, Vysvetlenie k článku 1, Ú. v. EÚ C 303, 14.12.2007, s. 17 – 35.
[18] Rozsudok SDEÚ vo veci C-601/15, bod 52.
[19] Rozsudok SDEÚ vo veci C-400/10, RoC 2010 I-08965, bod 55.
[20] Rozsudok SDEÚ vo veci C-408/03, RoC 2006 I-02647, bod 68.
[21] Rozsudok SDEÚ vo veci C-203/15 - Tele2 Sverige, bod 101 s odkazom na rozsudok SDEÚ vo veci C-293/12 a C-594/12, bod 39.
[22] Rozsudok SDEÚ vo veci C-512/18, La Quadrature du Net, bod 209 a nasl.
[23] Rozsudok SDEÚ vo veci C-594/12, bod 40.

#### *3.1.3.3 Legitímny cieľ*

47. Ako už bolo vysvetlené v bode 3.1.3., obmedzenia základných práv musia skutočne zodpovedať cieľom všeobecného záujmu, ktoré sú uznané Európskou úniou alebo spĺňať potrebu ochrany práv a slobôd iných.

48. Európska únia uznáva ciele uvedené v článku 3 Zmluvy o Európskej únii, ako aj iné záujmy chránené osobitnými ustanoveniami zmlúv[24], t. j. okrem iného priestor slobody, bezpečnosti a spravodlivosti, predchádzanie trestnej činnosti a boj proti nej. Únia by mala vo svojich vzťahoch so zvyškom sveta prispievať k mieru a bezpečnosti a ochrane ľudských práv.

49. Potreba chrániť práva a slobody iných sa vzťahuje na práva osôb, ktoré sú chránené právom Európskej únie alebo jej členských štátov. Posúdenie sa musí vykonať s cieľom zosúladiť požiadavky ochrany príslušných práv a dosiahnuť medzi nimi spravodlivú rovnováhu [25].

#### *3.1.3.4 Test nevyhnutnosti a primeranosti*

50. Ak ide o zásahy do základných práv, rozsah voľnej úvahy vnútroštátneho zákonodarcu a zákonodarcu Únie môže v konečnom dôsledku byť obmedzený. Závisí to od viacerých faktorov vrátane dotknutej oblasti, povahy predmetného práva zaručeného Chartou, povahy a závažnosti zásahu a cieľa sledovaného zásahom[26]. Legislatívne opatrenia musia byť primerané na dosiahnutie legitímnych cieľov sledovaných predmetnou právnou úpravou. Okrem toho opatrenie nesmie prekročiť hranice toho, čo je primerané a nevyhnutné na dosiahnutie týchto cieľov[27]. Cieľ všeobecného záujmu - nech už je akokoľvek zásadný - sám osebe neodôvodňuje obmedzenie základného práva[28].

51. Podľa ustálenej judikatúry SDEÚ výnimky a obmedzenia ochrany osobných údajov musia pôsobiť len v rámci toho, čo je úplne nevyhnutné[29]. Znamená to aj, že na dosiahnutie tohto cieľa nie sú k dispozícii žiadne menej rušivé prostriedky. Je potrebné dôkladne identifikovať a posúdiť možné alternatívy, ako napríklad – v závislosti od daného účelu – dodatočný personál, častejšia policajná kontrola alebo dodatočné pouličné osvetlenie. Legislatívne opatrenia by mali rozlišovať medzi osobami, na ktoré sa vzťahujú a zameriavať sa na príslušné osoby vzhľadom na cieľ, napr. boj proti závažnej trestnej činnosti. Ak sa vzťahuje na všetky osoby všeobecným spôsobom bez takéhoto rozlišovania, obmedzenia alebo výnimky, prehlbuje sa tým zásah[30]. Zásah sa prehlbuje aj v prípade, ak sa spracúvanie údajov týka významnej časti obyvateľstva[31].

52. Ochrana osobných údajov vyplývajúca z výslovnej povinnosti stanovenej v článku 8 ods. 1 Charty má mimoriadny význam pre právo na rešpektovanie súkromného života zakotvené v jej článku 7[32]. V právnych predpisoch sa musia stanoviť jasné a presné pravidlá upravujúce rozsah a uplatnenie

---

[24] Vysvetlenia k Charte základných práv, hlava I, Vysvetlenie k článku 52, Ú. v. EÚ C 303, 14.12.2007, s. 17 – 35.
[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31 – 32.
[26] Rozsudok SDEÚ vo veci C-594/12, bod 47 s týmito zdrojmi: pozri analogicky, pokiaľ ide o článok 8 EDĽP, ESĽP, S. a Marper/Spojené kráľovstvo [VK], č. 30562/04 a 30566/04, § 102, EDĽP 2008-V.
[27] Rozsudok SDEÚ vo veci C-594/12, bod 46 s týmito zdrojmi: Vec C-343/09 Afton Chemical EU:C:2010:419, bod 45; Volker und Markus Schecke a Eifert EU:C:2010:662, bod 74; veci C-581/10 a C-629/10 Nelson a i. EÚ:C:2012:657, bod 71; vec C-283/11 Sky Österreich EU:C:2013:28, bod 50; a vec C-101/12 Schaible EU:C:2013:661, bod 29.
[28] Rozsudok SDEÚ vo veci C-594/12, bod 51.
[29] Rozsudok SDEÚ vo veci C-594/12, bod 52, s týmito zdrojmi: vec C-473/12 IPI, EU:C:2013:715, bod 39 a citovaná judikatúra.
[30] Rozsudok SDEÚ vo veci C-594/12, bod 57.
[31] Rozsudok SDEÚ vo veci C-594/12, bod 56.
[32] Rozsudok SDEÚ vo veci C-594/12, bod 53.

predmetného opatrenia a ukladajúce minimálne požiadavky spôsobom, aby osoby, ktorých údaje boli uchované, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje proti rizikám zneužitia, ako aj proti akémukoľvek nezákonnému prístupu a akémukoľvek nezákonnému použitiu týchto údajov[33]. Potreba takýchto záruk je o to väčšia, ak osobné údaje podliehajú automatickému spracúvaniu a ak existuje značné riziko nezákonného prístupu k údajom[34]. Okrem toho interné alebo externé, napr. justičné, povolenie na zavedenie TRT môže takisto prispieť ako záruka, pričom sa môže preukázať, že je nevyhnutné v určitých prípadoch závažného zasahovania.[35]

53. Stanovené pravidlá musia byť prispôsobené konkrétnej situácii, napr. množstvu spracúvaných údajov, povahe údajov[36] a riziku nezákonného prístupu k údajom. Vyžaduje si to pravidlá, ktoré by slúžili najmä na jasné a prísne riadenie ochrany a bezpečnosti predmetných údajov s cieľom zabezpečiť ich úplnú integritu a dôvernosť[37].

54. Pokiaľ ide o vzťah medzi prevádzkovateľom a sprostredkovateľom, nemalo by sa sprostredkovateľom povoliť, aby pri stanovení úrovne bezpečnosti, ktorú uplatňujú na osobné údaje, zohľadnili len ekonomické úvahy; mohlo by to ohroziť dostatočne vysokú úroveň ochrany[38].

55. Právny akt musí stanoviť hmotnoprávne a procesné podmienky a objektívne kritériá, na základe ktorých sa vymedzí prístup príslušných orgánov k údajom a ich neskoršie použitie. Na účely prevencie, odhaľovania alebo trestného stíhania by sa príslušné trestné činy museli považovať za dostatočne závažné na to, aby odôvodňovali rozsah a závažnosť týchto zásahov do základných práv zakotvených napríklad v článkoch 7 a 8 Charty[39].

56. Údaje sa musia spracúvať spôsobom, ktorý zabezpečuje uplatniteľnosť a účinnosť pravidiel EÚ o ochrane údajov; najmä pravidiel stanovených v článku 8 Charty, v ktorom sa uvádza, že dodržiavanie požiadaviek na ochranu a bezpečnosť podlieha kontrole nezávislého orgánu. Zemepisné miesto, kde sa spracúvanie uskutočňuje, môže byť v takejto situácii relevantné[40].

57. Pokiaľ ide o rôzne kroky spracúvania osobných údajov, malo by sa rozlišovať medzi kategóriami údajov na základe ich možnej užitočnosti na účely sledovaného cieľa alebo podľa dotknutých osôb[41]. Určenie podmienok spracúvania, napríklad určenie doby uchovávania, musí vychádzať z objektívnych kritérií, aby sa zabezpečilo, že zásah bude obmedzený na to, čo je úplne nevyhnutné[42].

58. Na základe každej situácie musí posúdenie nevyhnutnosti a primeranosti identifikovať a zvážiť všetky dôsledky, ktoré patria do rozsahu pôsobnosti iných základných práv, ako je ľudská dôstojnosť podľa

[33] Rozsudok SDEÚ vo veci C-594/12, bod 54, s týmito zdrojmi: pozri analogicky, pokiaľ ide o článok 8 EDĽP, ESĽP, Liberty a iní/Spojené kráľovstvo, 1. júla 2008, č. 58243/00, bod 62 a 63; Rotaru/Rumunsko, bod 57 až 59, a S. a Marper/Spojené kráľovstvo, bod 99.
[34] Rozsudok SDEÚ vo veci C-594/12, bod 55, s týmito zdrojmi: pozri analogicky, pokiaľ ide o článok 8 EDĽP, S. a Marper/Spojené kráľovstvo, bod 103, a M. K./Francúzsko, 18. apríla 2013, č. 19522/09, bod 35.
[35] ESĽP, Szabó a Vissy/Maďarsko, body 73 – 77.
[36] Pozri aj zvýšené požiadavky na technické a organizačné opatrenia pri spracúvaní osobitných kategórií údajov, článok 29 ods. 1 LED.
[37] Rozsudok SDEÚ vo veci C-594/12, bod 66.
[38] Rozsudok SDEÚ vo veci C-594/12, bod 67.
[39] Rozsudok SDEÚ vo veci C-594/12, bod 60 a 61.
[40] Rozsudok SDEÚ vo veci C-594/12, bod 68.
[41] Rozsudok SDEÚ vo veci C-594/12, bod 63.
[42] Rozsudok SDEÚ vo veci C-594/12, bod 64.

článku 1 Charty, sloboda myslenia, svedomia a náboženského vyznania podľa článku 10 Charty, sloboda prejavu podľa článku 11 Charty, ako aj sloboda zhromažďovania a združovania podľa článku 12 Charty.

59. Okrem toho je potrebné považovať za závažnú skutočnosť, že ak sa údaje systematicky spracúvajú bez vedomia dotknutých osôb, môže to viesť k všeobecnému pocitu neustáleho sledovania[43]. To môže viesť k odstrašujúcim účinkom vo vzťahu k niektorým alebo všetkým dotknutým základným právam.

60. S cieľom uľahčiť a uviesť do praxe posudzovanie nevyhnutnosti a primeranosti legislatívnych opatrení týkajúcich sa rozpoznávania tváre v oblasti presadzovania práva by mohli vnútroštátni zákonodarcovia a zákonodarcovia Únie využiť dostupné praktické nástroje určené špeciálne na túto úlohu. Mohol by sa použiť najmä súbor nástrojov v oblasti nevyhnutnosti a primeranosti[44], ktorý poskytuje Európsky dozorný úradník pre ochranu údajov.

#### *3.1.3.5 Článok 52 ods. 3, článok 53 Charty (úroveň ochrany aj v súvislosti s Európskym dohovorom o ľudských právach)*

61. Podľa článku 52 ods. 3 a článku 53 Charty zmysel a rozsah týchto práv podľa Charty, ktoré zodpovedajú právam zaručeným v EDĽP, musí byť rovnaký ako zmysel a rozsah práv ustanovených v EDĽP. Zatiaľ čo najmä v prípade článku 7 Charty možno nájsť ekvivalent v EDĽP, pre článok 8 Charty to neplatí[45]. Článok 52 ods. 3 Charty nebráni tomu, aby právo Únie poskytovalo širší rozsah ochrany. Keďže EDĽP nepredstavuje právny nástroj, ktorý bol formálne začlenený do práva Únie, právne predpisy EÚ sa musia vykonávať s ohľadom na základné práva podľa Charty[46].

62. Podľa článku 8 EDĽP štátny orgán nemôže do výkonu tohto práva na rešpektovanie súkromného a rodinného života zasahovať s výnimkou prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom alebo zločinnosti, ochrany zdravia alebo morálky alebo na ochranu práv a slobôd iných.

63. EDĽP okrem toho stanovuje normy týkajúce sa spôsobu, akým možno uplatňovať obmedzenia. Jednou zo základných požiadaviek, okrem zásad právneho štátu, je predvídateľnosť. Na splnenie požiadavky predvídateľnosti musia byť pojmy v právnych predpisoch dostatočne jasné na to, aby jednotlivcov primerane informovali o tom, za akých okolností a podmienok sú orgány verejnej moci oprávnené uchýliť sa k takýmto opatreniam[47]. Túto požiadavku uznáva aj SDEÚ a právne predpisy EÚ o ochrane údajov (pozri oddiel 3.2.1.1).

64. V nadväznosti na práva uvedené v článku 8 EDĽP sa musia plne rešpektovať aj ustanovenia Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov[48]. Napriek tomu je potrebné vziať do úvahy, že tieto ustanovenia predstavujú len minimálny štandard vzhľadom na prevládajúce právne predpisy Únie.

---

[43] Rozsudok SDEÚ vo veci C-594/12, bod 37.

[44] Európsky dozorný úradník pre ochranu údajov: Posúdenie nevyhnutnosti opatrení, ktoré obmedzujú základné právo na ochranu osobných údajov: Súbor nástrojov (11.4.2017); Európsky dozorný úradník pre ochranu údajov: Usmernenia EDPS o posudzovaní primeranosti opatrení, ktorými sa obmedzujú základné práva na ochranu osobných údajov (19.12.2019).

[45] Rozsudok SDEÚ vo veci C-203/15, Tele2 Sverige, bod 129.

[46] Rozsudok SDEÚ vo veci C-311/18, bod 99.

[47] Rozsudok ESĽP vo veci Copland/Spojené kráľovstvo, 3.4.2007, sťažnosť č. 62617/00, bod 46.

[48] ETS č. 108.

## 3.2 Osobitný právny rámec – smernica o presadzovaní práva

65. V LED sa stanovuje určitý rámec týkajúci sa používania TRT. V prvom rade sa v článku 3 bode 13 LED vymedzuje pojem „biometrické údaje“[49]. Podrobnosti pozri v časti 2.1 vyššie. Po druhé, v článku 8 ods. 2 sa objasňuje, že na to, aby bolo každé spracúvanie zákonné, musí byť – okrem toho, že je nevyhnutné na účely stanovené v článku 1 ods. 1 LED – upravené v práve členského štátu, v ktorom sa stanovujú aspoň ciele spracúvania, osobné údaje, ktoré sa majú spracúvať, a účel spracúvania. Ďalšími ustanoveniami osobitného významu, pokiaľ ide o biometrické údaje, sú články 10 a 11 LED. Článok 10 sa musí vykladať v spojení s článkom 8 LED[50]. Zásady spracúvania osobných údajov stanovené v článku 4 LED by sa mali vždy dodržiavať a akékoľvek posúdenie možného biometrického spracúvania prostredníctvom TRT by sa malo riadiť týmito zásadami.

### 3.2.1 Spracúvanie osobitných kategórií údajov na účely presadzovania práva

66. Podľa článku 10 LED spracúvanie osobitných kategórií údajov, ako sú biometrické údaje, je možné len vtedy, ak je úplne nevyhnutné a podlieha primeraným zárukám ochrany práv a slobôd dotknutej osoby. Okrem toho je povolené len vtedy, ak to povoľuje právo Únie alebo členského štátu, na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby, alebo ak sa takéto spracúvanie týka údajov, ktoré dotknutá osoba preukázateľne sprístupnila. Toto všeobecné ustanovenie zdôrazňuje citlivosť spracúvania osobitných kategórií údajov.

#### *3.2.1.1 Povolené právom Únie alebo členského štátu*

67. Pokiaľ ide o potrebný typ legislatívneho opatrenia, v odôvodnení 33 LED sa uvádza, že „ak sa v tejto smernici odkazuje na právo členského štátu, právny základ alebo legislatívne opatrenie, nemusí sa tým nevyhnutne vyžadovať legislatívny akt prijatý parlamentom, bez toho, aby boli dotknuté požiadavky vyplývajúce z ústavného poriadku dotknutého členského štátu.“[51]

68. Podľa článku 52 ods. 1 Charty musí byť akékoľvek obmedzenie výkonu práv a slobôd uznaných v Charte „ustanovené zákonom“. Korešponduje to s výrazom „v súlade so zákonom“ uvedeným v článku 8 ods. 2 EDĽP, čo neznamená len súlad s uplatniteľnými právnymi predpismi, ale súvisí to aj s kvalitou zákona, bez toho, aby bola dotknutá povaha daného aktu, v ktorom sa vyžaduje súlad so zásadami právneho štátu.

69. V odôvodnení 33 LED sa ďalej uvádza, že „[t]akéto právo členského štátu, právny základ alebo legislatívne opatrenie by však mali byť jasné a presné a ich uplatňovanie predvídateľné pre tých, na ktorých sa vzťahujú, ako to vyžaduje judikatúra Súdneho dvora a Európskeho súdu pre ľudské práva. V práve členského štátu, ktorým sa upravuje spracúvanie osobných údajov v rámci rozsahu pôsobnosti tejto smernice, by sa mali uviesť aspoň ciele, osobné údaje, ktoré sa majú spracúvať, účely spracúvania a postupy na zachovanie integrity a dôvernosti osobných údajov a postupy na ich likvidáciu.“

70. Znenia vnútroštátnych právnych predpisov majú byť dostatočne jasné na to, aby dali dotknutým osobám náležitým spôsobom najavo, za akých okolností a podmienok sú prevádzkovatelia oprávnení uchýliť sa k akýmkoľvek obmedzeniam. To zahŕňa možné podmienky na spracúvanie, ako sú osobitné druhy dôkazov, ako aj nevyhnutnosť súdneho alebo vnútorného povolenia. Príslušné právne predpisy

[49] Článok 3 bod 13 LED: „Biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre [facial images] alebo daktyloskopické údaje.

[50] WP258, Stanovisko k niektorým kľúčovým otázkam smernice o presadzovaní práva [(EÚ) 2016/680], s. 7.

[51] Typ zvažovaných legislatívnych opatrení musí byť v súlade s právom EÚ alebo s vnútroštátnymi právnymi predpismi. V závislosti od miery zásahu obmedzenia by sa na vnútroštátnej úrovni mohlo vyžadovať osobitné legislatívne opatrenie zohľadňujúce úroveň tejto normy.

môžu byť technologicky neutrálne, pokiaľ dostatočne riešia osobitné riziká a charakteristiky spracúvania osobných údajov v systémoch TRT. V súlade s LED a judikatúrou Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva je skutočne nevyhnutné, aby boli legislatívne opatrenia, ktorých cieľom je poskytnúť právny základ pre opatrenie na rozpoznávanie tváre, predvídateľné pre dotknuté osoby.

71. Na legislatívne opatrenie sa nemožno odvolávať ako na zákon, ktorým sa povoľuje spracúvanie biometrických údajov prostredníctvom TRT na účely presadzovania práva, ak ide len o transpozíciu všeobecného ustanovenia podľa článku 10 LED.

72. Okrem biometrických údajov sa v článku 10 LED upravuje spracúvanie ďalších osobitných kategórií údajov, ako sú sexuálna orientácia, politické názory a náboženské presvedčenie, čím sa pokrýva široký rozsah spracúvania. Okrem toho by v takomto ustanovení chýbali osobitné požiadavky poukazujúce na okolnosti a podmienky, za ktorých by orgány presadzovania práva boli oprávnené uchýliť sa k používaniu technológie rozpoznávania tváre. Vzhľadom na odkazy na iné druhy údajov a výslovnú potrebu osobitných záruk bez ďalších špecifikácií, vnútroštátne ustanovenie, ktorým sa transponuje článok 10 LED do vnútroštátneho práva – s podobne všeobecným a abstraktným znením – sa nemôže považovať za právny základ pre spracúvanie biometrických údajov, ktoré zahŕňa rozpoznávanie tváre, pretože by mu chýbala presnosť a predvídateľnosť. V súlade s článkom 28 ods. 2 alebo článkom 46 ods. 1 písm. c) LED pred tým, ako zákonodarca vytvorí nový právny základ pre akúkoľvek formu spracúvania biometrických údajov pomocou rozpoznávania tváre, mal by sa obrátiť na vnútroštátny dozorný orgán pre ochranu údajov.

#### *3.2.1.2 Úplná nevyhnutnosť*

73. Spracúvanie možno považovať za „úplne nevyhnutné“ len vtedy, ak zásah do ochrany osobných údajov a jeho obmedzenia sú obmedzené na to, čo je absolútne nevyhnutné[52]. Doplnenie pojmu „úplne“ znamená, že úmyslom zákonodarcu bolo, aby sa spracúvanie osobitných kategórií údajov uskutočňovalo len za podmienok, ktoré sú ešte prísnejšie ako podmienky nevyhnutnosti (pozri bod 3.1.3.4 vyššie). Táto požiadavka by sa mala vykladať ako bezpodmienečne nutná. Obmedzuje priestor na voľnú úvahu, ktorý je orgánu presadzovania práva povolený v rámci testu nevyhnutnosti, na absolútne minimum. V súlade s ustálenou judikatúrou SDEÚ je podmienka „úplnej nevyhnutnosti“ takisto úzko spojená s požiadavkou objektívnych kritérií s cieľom vymedziť okolnosti a podmienky, za ktorých sa môže spracúvanie vykonávať, čím sa vylučuje akékoľvek spracúvanie všeobecnej alebo systematickej povahy[53].

#### *3.2.1.3 Preukázateľné sprístupnenie*

74. Pri posudzovaní toho, či sa spracúvanie týka údajov, ktoré preukázateľne sprístupnila dotknutá osoba, treba pripomenúť, že fotografia ako taká sa systematicky nepovažuje za biometrické údaje[54]. Preto skutočnosť, že dotknutá osoba preukázateľne sprístupnila fotografiu, neznamená, že sa za preukázateľne sprístupnené považujú súvisiace biometrické údaje, ktoré možno získať z fotografie osobitnými technickými prostriedkami.

---

[52] Ustálená judikatúra k základnému právu na rešpektovanie súkromného života, pozri rozsudok SDEÚ vo veci C-73/07, bod 56 (Satakunnan Markkinapörssi a Satamedia); rozsudok SDEÚ vo veci C-92/09 a C-93/09 bod 77 (Schecke a Eifert); rozsudok SDEÚ vo veci C-594/12, bod 52 (Digital Rights); rozsudok SDEÚ vo veci C-362/14, bod 92 (Schrems).

[53] Rozsudok SDEÚ vo veci C-623/17, bod 78.

[54] Podľa odôvodnenia 51 všeobecného nariadenia o ochrane údajov: „spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby.“

75. Pokiaľ ide o osobné údaje vo všeobecnosti, na to, aby sa biometrické údaje považovali za preukázateľne sprístupnené dotknutou osobou, dotknutá osoba musela zámerne sprístupniť a zverejniť biometrický vzor (a nie iba snímka tváre) prostredníctvom otvoreného zdroja. Ak biometrické údaje poskytuje tretia strana, nemožno sa domnievať, že dotknutá osoba údaje preukázateľne sprístupnila.

76. Okrem toho nestačí interpretovať správanie dotknutej osoby, aby sa dalo usúdiť, že biometrické údaje boli preukázateľne sprístupnené. Napríklad v prípade sociálnych sietí alebo online platforiem sa EDPB domnieva, že skutočnosť, že dotknutá osoba nespustila alebo nenastavila konkrétne prvky ochrany osobných údajov, nestačí na domnienku, že táto dotknutá osoba preukázateľne sprístupnila svoje osobné údaje a že tieto údaje (napr. fotografie) možno spracúvať do biometrických vzorov a použiť na účely identifikácie bez súhlasu dotknutej osoby. Všeobecnejšie povedané, predvolené nastavenia služby, napr. zverejňovanie vzorov, alebo absencia možnosti voľby, napr. zverejňovanie vzorov bez toho, aby používateľ mohol toto nastavenie zmeniť, by sa v žiadnom prípade nemali chápať ako preukázateľne sprístupnené údaje.

### 3.2.2 Automatizované individuálne rozhodovanie vrátane profilovania

77. V článku 11 ods. 1 LED sa stanovuje povinnosť členských štátov všeobecne zakázať rozhodnutia založené výlučne na automatizovanom spracúvaní vrátane profilovania, ktoré má pre dotknutú osobu nepriaznivé právne účinky alebo významné dôsledky. Ako výnimka z tohto všeobecného zákazu môže byť takéto spracúvanie možné len vtedy, ak je povolené právom Únie alebo členského štátu, ktorému prevádzkovateľ podlieha a ktoré poskytuje primerané záruky pre práva a slobody dotknutej osoby, aspoň právo na ľudský zásah zo strany prevádzkovateľa. Môže sa používať len reštriktívne. Táto podmienka sa vzťahuje na bežné (t. j. nie osobitné) kategórie osobných údajov. Na výnimku podľa článku 11 ods. 2 LED sa vzťahuje ešte prísnejšia podmienka a obmedzenejšie používanie. Opätovne zdôrazňuje, že rozhodnutia podľa prvého odseku nesmú byť založené na osobitných kategóriách údajov, t. j. najmä nie na biometrických údajoch na účely jedinečnej identifikácie fyzickej osoby. Výnimku možno stanoviť len vtedy, ak sú zavedené vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej fyzickej osoby. Táto výnimka sa musí vykladať ako doplnenie článku 10 LED a s ohľadom na toto ustanovenie.

78. V závislosti od systému TRT nemusí ani ľudský zásah pri posudzovaní výsledkov TRT ako taký nevyhnutne poskytovať dostatočnú záruku dodržiavania práv jednotlivcov, a najmä práva na ochranu osobných údajov, vzhľadom na možné skreslenie a chybu, ktorá môže vyplývať zo samotného spracúvania. Okrem toho sa ľudský zásah môže považovať za záruku len vtedy, ak osoba, ktorá zásah vykonáva, môže počas ľudského zásahu kriticky spochybniť výsledky TRT. Je nevyhnutné umožniť tejto osobe pochopiť systém TRT a jeho obmedzenia, ako aj správne interpretovať jeho výsledky. Takisto je potrebné vytvoriť pracovné miesto a organizáciu, ktoré budú pôsobiť proti účinkom nadmerného dôverovania automatizácii a budú predchádzať podpore nekritickej akceptácie výsledkov, napr. z dôvodu časového tlaku, náročných postupov, potenciálne škodlivých účinkov na kariéru atď.

79. Podľa článku 11 ods. 3 LED sa profilovanie, ktoré vedie k diskriminácii fyzických osôb na základe osobitných kategórií osobných údajov, ako sú biometrické údaje, zakazuje v súlade s právom Únie. Podľa článku 3 ods. 4 LED „profilovanie“ je akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom. Pri zvažovaní, či sa predpokladajú vhodné opatrenia na ochranu práv a slobôd dotknutej osoby a oprávnených záujmov dotknutej osoby, je potrebné mať na pamäti, že používanie TRT môže viesť k profilovaniu v závislosti od spôsobu a účelu,

na ktorý sa TRT používa. V súlade s právom Únie a článkom 11 ods. 3 LED je každopádne zakázané profilovanie, ktoré vedie k diskriminácii fyzických osôb na základe osobitných kategórií osobných údajov.

### 3.2.3 Kategórie dotknutých osôb

80. Článok 6 LED sa týka potreby rozlišovať medzi rôznymi kategóriami dotknutých osôb. Toto rozlíšenie sa musí vykonať v príslušných prípadoch a v najväčšej možnej miere. Musí sa prejaviť v spôsobe spracúvania údajov. Z príkladov uvedených v článku 6 LED možno vyvodiť, že spracúvanie osobných údajov musí spravidla spĺňať kritériá nevyhnutnosti a primeranosti aj vzhľadom na kategóriu dotknutých osôb[55]. Ďalej možno dospieť k záveru, že pokiaľ ide o dotknuté osoby, v prípade ktorých neexistuje žiadny dôkaz, z ktorého by mohlo vyplývať, že ich konanie by mohlo hoci len nepriamo alebo vzdialene súvisieť s legitímnym cieľom podľa LED, s najväčšou pravdepodobnosťou neexistuje odôvodnenie zásahu[56]. Ak nie je možné alebo uplatniteľné rozlišovanie podľa článku 6 LED, pri posudzovaní nevyhnutnosti a primeranosti zásahu sa musí prísne zvážiť výnimka z pravidla článku 6 LED. Rozlišovanie medzi rôznymi kategóriami dotknutých osôb sa javí ako základná požiadavka, pokiaľ ide o spracúvanie osobných údajov zahŕňajúce rozpoznávanie tváre, a to aj vzhľadom na možné falošne pozitívne alebo falošne negatívne výsledky, ktoré môžu mať významný vplyv na dotknuté osoby, ako aj na priebeh vyšetrovania.

81. Ako už bolo uvedené, pri vykonávaní práva Únie sa musia dodržiavať ustanovenia Charty základných práv Európskej únie, pozri článok 52 Charty. Rámec a kritériá, ktoré stanovuje LED, sa preto majú vykladať vo svetle Charty. Právne akty EÚ a jej členských štátov nesmú toto opatrenie porušovať a musia zabezpečiť plný účinok Charty.

### 3.2.4 Práva dotknutej osoby

82. EDPB už poskytol usmernenia o právach dotknutých osôb podľa všeobecného nariadenia o ochrane údajov v rôznych aspektoch[57]. V LED sa stanovujú podobné práva dotknutých osôb a všeobecné usmernenia k tejto téme sú uvedené v stanovisku pracovnej skupiny zriadenej podľa článku 29, ktoré schválil EDPB[58]. Za určitých okolností LED umožňuje určité obmedzenia týchto práv. Parametre takýchto obmedzení budú podrobnejšie rozpracované v oddiele 3.2.4.6. „Oprávnené obmedzenia práv dotknutej osoby“.

83. Hoci sa všetky práva dotknutej osoby uvedené v kapitole III LED prirodzene uplatňujú aj na spracúvanie osobných údajov prostredníctvom technológie rozpoznávania tvárí (TRT), nasledujúca kapitola sa zameriava na niektoré práva a aspekty, ktoré môžu byť predmetom osobitného záujmu o usmernenie. Táto kapitola a v nej obsiahnutá analýza sú podmienené tým, že príslušné spracúvanie TRT splnilo právne požiadavky, ako je opísané v predchádzajúcej kapitole.

84. Vzhľadom na povahu spracúvania osobných údajov prostredníctvom TRT (spracúvanie osobitných kategórií osobných údajov často bez akejkoľvek zjavnej interakcie s dotknutou osobou) musí prevádzkovateľ starostlivo zvážiť, ako (alebo či dokáže) spĺňať požiadavky LED pred začatím akéhokoľvek spracúvania pomocou TRT. Mal by dôkladne analyzovať najmä:

- kto sú dotknuté osoby (často aj iné, ako tie, ktoré sú hlavným cieľom na účely spracúvania),

[55] Pozri aj rozsudok SDEÚ vo veci C-594/12, bod 56 - 59.
[56] Pozri aj rozsudok SDEÚ vo veci C-594/12, bod 58.
[57] Pozri napríklad Usmernenia EDPB 1/2022 k právam dotknutých osôb - právo na prístup a Usmernenia EDPB 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení.
[58] WP258, Stanovisko k niektorým kľúčovým otázkam smernice o presadzovaní práva [(EÚ) 2016/680].

- ako sú dotknuté osoby informované o spracúvaní pomocou TRT (pozri oddiel 3.2.4.1),
- ako môžu dotknuté osoby uplatniť svoje práva (v tomto prípade môže byť obzvlášť náročné vykonávať práva na informácie a prístup, ako aj práva na opravu alebo obmedzenie v prípade, že sa TRT používa na všetky overenia okrem overenia jedna k jednej v priamom kontakte s dotknutou osobou).

#### *3.2.4.1 Sprostredkovanie práv a informácií dotknutým osobám v stručnej, zrozumiteľnej a ľahko dostupnej forme*

85. Pri TRT vyplývajú výzvy zo zabezpečovania toho, aby dotknuté osoby boli informované o spracúvaní svojich biometrických údajov. Je to obzvlášť náročné, ak OPP analyzuje prostredníctvom TRT videozáznam, ktorý pochádza od tretej strany alebo ho poskytla tretia strana, pretože OPP má len malú, a väčšinou žiadnu možnosť informovať dotknutú osobu v čase získania údajov (napr. formou oznamu na mieste). Akýkoľvek videozáznam, ktorý nie je relevantný pre vyšetrovanie (alebo účel spracúvania), by sa mal vždy odstrániť alebo anonymizovať (napr. rozmazaním bez možnosti spätného obnovenia údajov) pred nasadením akéhokoľvek spracúvania biometrických údajov, aby sa predišlo riziku nedodržania zásady minimalizácie podľa článku 4 ods. 1 písm. e) LED a informačných povinností podľa článku 13 ods. 2 LED. Prevádzkovateľ je zodpovedný za posúdenie toho, aké informácie by mohli byť dôležité pre dotknutú osobu pri uplatňovaní jej práv, a za zabezpečenie poskytnutia potrebných informácií. Účinný výkon práv dotknutej osoby závisí od toho, či prevádzkovateľ plní svoje informačné povinnosti.

86. V článku 13 ods. 1 LED sa stanovuje, aké minimálne informácie sa musia poskytnúť dotknutej osobe vo všeobecnosti. Tieto informácie sa môžu poskytovať prostredníctvom webovej stránky prevádzkovateľa, v tlačenej forme (napr. leták dostupný na požiadanie) alebo z iných, pre dotknutú osobu ľahko dostupných zdrojov. Prevádzkovateľ musí v každom prípade zabezpečiť, aby sa informácie účinne poskytovali aspoň v súvislosti s týmito prvkami:

- totožnosť a kontaktné údaje prevádzkovateľa vrátane zodpovednej osoby,
- účel spracúvania a že ide o spracúvanie prostredníctvom TRT,
- právo podať sťažnosť dozornému orgánu a kontaktné údaje takéhoto orgánu,
- právo požiadať o prístup k osobným údajom a o opravu alebo vymazanie osobných údajov a obmedzenie spracúvania osobných údajov.

87. Okrem toho v osobitných prípadoch vymedzených vo vnútroštátnom práve, ktoré by mali byť v súlade s článkom 13 ods. 2 LED[59], ako napríklad spracúvanie pomocou TRT, je potrebné poskytnúť tieto informácie priamo dotknutej osobe:

- právny základ spracúvania,
- informácie o tom, kde boli osobné údaje získané bez vedomia dotknutej osoby,
- doba uchovávania osobných údajov alebo ak to nie je možné, kritériá používané na určenie tejto doby,
- prípadne kategórie príjemcov osobných údajov (vrátane tretích krajín alebo medzinárodných organizácií).

[59] Napr. § 56 ods. 1 nemeckého spolkového zákona o ochrane údajov, v ktorom sa okrem iného uvádza, aké informácie je potrebné poskytnúť dotknutým osobám v súvislosti s utajenými operáciami.

88. Zatiaľ čo článok 13 ods. 1 LED sa týka všeobecných informácií sprístupnených verejnosti, článok 13 ods. 2 LED sa týka ďalších informácií, ktoré sa majú poskytnúť konkrétnej dotknutej osobe v osobitných prípadoch, napríklad ak sa údaje získavajú priamo od dotknutej osoby alebo nepriamo bez vedomia dotknutej osoby[60]. V článku 13 ods. 2 LED neexistuje jasné vymedzenie toho, čo sa myslí pod pojmom „osobitné prípady". Vzťahuje sa však na situácie, keď je potrebné, aby dotknuté osoby boli informované o spracúvaní, ktoré sa ich konkrétne týka, a aby im boli poskytnuté primerané informácie, aby mohli účinne uplatniť svoje práva. EDPB sa domnieva, že pri posudzovaní toho, či ide o „osobitný prípad", je potrebné zohľadniť niekoľko faktorov vrátane toho, či sa osobné údaje zhromažďujú bez vedomia dotknutej osoby, pretože to by bol jediný spôsob, ako umožniť dotknutým osobám účinne uplatňovať svoje práva. Ďalšími príkladmi „osobitných prípadov" by mohli byť prípady, keď sa osobné údaje ďalej spracúvajú v rámci medzinárodnej spolupráce v trestných veciach alebo v situácii, keď sa osobné údaje spracúvajú v rámci utajených operácií stanovených vo vnútroštátnom práve. Okrem toho z odôvodnenia 38 LED vyplýva, že ak sa rozhodovanie uskutočňuje výlučne na základe TRT, potom je potrebné informovať dotknuté osoby o vlastnostiach automatizovaného rozhodovania. To by tiež naznačovalo, že ide o osobitný prípad, keď by sa dotknutej osobe mali poskytnúť dodatočné informácie v súlade s článkom 13 ods. 2 LED[61].

89. Napokon treba poznamenať, že podľa článku 13 ods. 3 LED môžu členské štáty prijať legislatívne opatrenia, ktoré obmedzujú povinnosť poskytovať informácie v osobitných prípadoch na určité ciele. Platí to v takom rozsahu a dovtedy, kým takéto opatrenie predstavuje nevyhnutné a primerané opatrenie v demokratickej spoločnosti s náležitým ohľadom na základné práva a oprávnené záujmy dotknutej osoby.

#### *3.2.4.2 Právo na prístup*

90. Vo všeobecnosti má dotknutá osoba právo získať kladné alebo záporné potvrdenie o akomkoľvek spracúvaní svojich osobných údajov a v prípade kladnej odpovede aj prístup k samotným osobným údajom spolu s ďalšími informáciami, ako sa uvádza v článku 14 LED. V prípade TRT, ak sú biometrické údaje uložené a spojené s totožnosťou aj prostredníctvom alfanumerických údajov, malo by to príslušnému orgánu umožniť potvrdiť žiadosť o prístup na základe vyhľadávania podľa týchto alfanumerických údajov a bez toho, aby sa začalo ďalšie spracúvanie biometrických údajov iných osôb (t. j. vyhľadávanie pomocou TRT v databáze). Musí sa dodržiavať zásada minimalizácie údajov a nemalo by sa uchovávať viac údajov, ako je nevyhnutné vzhľadom na účel spracúvania.

#### *3.2.4.3 Právo na opravu osobných údajov*

91. Vzhľadom na to, že TRT neumožňuje absolútnu správnosť, je obzvlášť dôležité, aby prevádzkovatelia pozorne sledovali žiadosti o opravu osobných údajov. Môže sa stať, že dotknutá osoba bola na základe TRT zaradená do nesprávnej kategórie, napr. nesprávne zaradená do kategórie podozrivých na základe prvej domnienky o priebehu konania na videozázname. Riziká pre dotknuté osoby sú obzvlášť závažné, ak sa takéto nesprávne údaje uchovávajú v policajnej databáze a/alebo sa zdieľajú s inými subjektmi. Prevádzkovateľ musí príslušne opraviť uložené údaje a systémy TRT, pozri odôvodnenie 47 LED.

#### *3.2.4.4 Právo na výmaz*

92. TRT bude za väčšiny okolností – v prípade, že sa nepoužíva na overenie/autentifikáciu 1:1 - predstavovať spracúvanie veľkého počtu biometrických údajov dotknutých osôb. Je preto dôležité, aby prevádzkovateľ vopred zvážil obmedzenia jej účelu a nevyhnutnosti tak, aby sa žiadosť o vymazanie v

[60] WP258, Stanovisko k niektorým kľúčovým otázkam smernice o presadzovaní práva [(EÚ) 2016/680], s. 17 – 18

[61] Všimnite si rozdiel medzi slovami „sprístupniť dotknutej osobe" v článku 13 ods. 1 LED a „poskytnúť dotknutej osobe" v článku 13 ods. 2 LED. Podľa článku 13 ods. 2 LED musí prevádzkovateľ zabezpečiť, aby sa informácie dostali k dotknutej osobe, keď informácie uverejnené na webovom sídle nebudú postačovať.

súlade s článkom 16 LED mohla vybaviť bez zbytočného odkladu (keďže prevádzkovateľ musí okrem iného vymazať osobné údaje, ktoré sa spracúvajú nad rámec toho, čo umožňujú platné právne predpisy podľa článkov 4, 8 a 10 LED).

#### *3.2.4.5 Právo na obmedzenie*

93. V prípade, že dotknutá osoba napadne správnosť údajov a správnosť údajov nie je možné určiť (alebo keď osobné údaje musia byť uchovávané na účely budúceho dokazovania), prevádzkovateľ má povinnosť obmedziť osobné údaje tejto dotknutej osoby v súlade s článkom 16 LED. Je to obzvlášť dôležité, najmä ak ide o technológiu rozpoznávania tváre [založenú na algoritme (algoritmoch), a teda nikdy nezobrazujúcu definitívny výsledok] v situáciách, keď sa zhromažďuje veľké množstvo údajov a môže dochádzať k identifikácii s rôznou mierou správnosti a kvality. Pri nekvalitných videozáznamoch (napr. z miesta činu) sa zvyšuje riziko falošne pozitívnych výsledkov. Okrem toho, ak sa snímky tvárí v zozname sledovaných osôb pravidelne neaktualizujú, zvyšuje sa aj riziko falošne pozitívnych alebo falošne negatívnych výsledkov. V osobitných prípadoch, keď údaje nemožno vymazať z dôvodu, že existujú opodstatnené dôvody domnievať sa, že vymazanie by mohlo ovplyvniť oprávnené záujmy dotknutej osoby, údaje by sa namiesto toho mali obmedziť a spracúvať len na účel, ktorý bráni ich vymazaniu (pozri odôvodnenie 47 LED).

#### *3.2.4.6 Oprávnené obmedzenia práv dotknutej osoby*

94. Pokiaľ ide o informačné povinnosti prevádzkovateľa a právo dotknutých osôb na prístup k údajom, obmedzenia sú povolené, len pokiaľ sú stanovené v právnych predpisoch, ktoré musia predstavovať nevyhnutné a primerané opatrenie v demokratickej spoločnosti s náležitým ohľadom na základné práva a oprávnené záujmy danej fyzickej osoby (pozri článok 13 ods. 3, článok 13 ods. 4, článok 15 a článok 16 ods. 4 LED). Keď sa TRT používa na účely presadzovania práva, možno očakávať, že sa bude používať za okolností, v ktorých by bolo vzhľadom na sledovaný cieľ nežiadúce informovať dotknutú osobu alebo umožniť prístup k údajom. To by sa vzťahovalo napríklad na policajné vyšetrovanie trestného činu alebo na ochranu národnej bezpečnosti alebo verejnej bezpečnosti.

95. Právo na prístup neznamená automaticky prístup ku všetkým informáciám, napr. v trestnom konaní, ktoré zahŕňa osobné údaje osoby. Realistickým príkladom toho, kedy môžu byť povolené obmedzenia tohto práva, by mohlo byť prebiehajúce vyšetrovanie trestného činu.

#### *3.2.4.7 Uplatňovanie práv prostredníctvom dozorného orgánu*

96. V prípadoch, keď existujú legitímne obmedzenia výkonu práv podľa kapitoly III LED, dotknutá osoba môže požiadať orgán pre ochranu osobných údajov, aby v jej mene uplatnil jej práva, a to prostredníctvom kontroly zákonnosti spracúvania u prevádzkovateľa. Prevádzkovateľ je povinný informovať dotknutú osobu o takejto možnosti uplatniť jej práva [pozri článok 17 LED a článok 46 ods. 1 písm. g) LED]. V prípade TRT to znamená, že prevádzkovateľ musí zabezpečiť, aby boli zavedené vhodné opatrenia na vybavenie takejto žiadosti, napr. umožnenie vyhľadávania zaznamenaného materiálu za predpokladu, že dotknutá osoba poskytne dostatočné informácie na lokalizáciu svojich osobných údajov.

### 3.2.5 Ďalšie právne požiadavky a záruky

#### *3.2.5.1 Článok 27 Posúdenie vplyvu na ochranu údajov*

97. Posúdenie vplyvu na ochranu údajov (DPIA) pred použitím TRT je povinnou požiadavkou, pretože tento typ spracúvania, najmä s použitím nových technológií, a pri zohľadnení povahy, rozsahu, kontextu a účelov spracúvania môže viesť k vysokému riziku pre práva a slobody fyzických osôb. Vzhľadom na to, že používanie TRT zahŕňa systematické automatické spracúvanie osobitných kategórií údajov, mohlo by sa predpokladať, že v takýchto prípadoch by prevádzkovateľ spravidla bol povinný vykonať posúdenie vplyvu na ochranu údajov. Posúdenie vplyvu na ochranu údajov by malo obsahovať aspoň

všeobecný opis plánovaných spracovateľských operácií, posúdenie nevyhnutnosti a primeranosti spracovateľských operácií vzhľadom na účely, hodnotenie rizík pre práva a slobody dotknutých osôb, plánované opatrenia na riešenie týchto rizík, záruky, bezpečnostné opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu. EDPB odporúča zverejniť výsledky takýchto posúdení alebo aspoň hlavné zistenia a závery DPIA ako opatrenie na zvýšenie dôvery a transparentnosti[62].

#### *3.2.5.2 Článok 28 Predchádzajúca konzultácia s dozorným orgánom*

98. Podľa článku 28 LED musí prevádzkovateľ alebo sprostredkovateľ pred spracúvaním konzultovať s dozorným orgánom, ak: a) je z posúdenia vplyvu na ochranu údajov zrejmé, že toto spracúvanie by viedlo k vysokému riziku, ak by prevádzkovateľ neprijal opatrenia na zmiernenie tohto rizika, alebo b) sa s typom spracúvania, najmä s využitím nových technológií, mechanizmov alebo postupov, spája vysoké riziko pre práva a slobody dotknutých osôb. Ako už bolo vysvetlené v oddiele 2.3. týchto usmernení, EDPB sa domnieva, že väčšina prípadov zavedenia a používania TRT sa vo svojej podstate vyznačuje vysokým rizikom pre práva a slobody dotknutých osôb. Okrem posúdenia vplyvu na ochranu údajov by preto orgán, ktorý zavádza TRT, mal pred zavedením systému konzultovať s príslušným dozorným orgánom.

#### *3.2.5.3 Článok 29 Bezpečnosť spracúvania*

99. Jedinečná povaha biometrických údajov neumožňuje, aby ich dotknutá osoba zmenila, ak dôjde k ich ohrozeniu, napr. v dôsledku porušenia ochrany údajov. Preto by mal príslušný orgán, ktorý zavádza a/alebo používa TRT, venovať osobitnú pozornosť bezpečnosti spracúvania v súlade s článkom 29 LED. Orgán presadzovania práva by mal predovšetkým zabezpečiť, aby systém spĺňal príslušné normy a mal by zaviesť opatrenia na ochranu biometrických vzorov[63]. Táto povinnosť je ešte dôležitejšia, ak orgán presadzovania práva využíva externého poskytovateľa služieb (sprostredkovateľa).

#### *3.2.5.4 Článok 20 Špecificky navrhnutá a štandardná ochrana údajov*

100. Cieľom špecificky navrhnutej a štandardnej ochrany údajov v súlade s článkom 20 LED je zabezpečiť, aby boli zásady a záruky ochrany údajov, ako je minimalizácia údajov a obmedzenie uchovávania, súčasťou technológie prostredníctvom vhodných technických a organizačných opatrení, ako je pseudonymizácia, a to ešte pred začiatkom spracúvania osobných údajov, a že sa budú uplatňovať počas celého jej životného cyklu. Vzhľadom na súvisiace vysoké riziko pre práva a slobody fyzických osôb by výber takýchto opatrení nemal závisieť výlučne od ekonomických úvah[64], ale mal by sa namiesto toho zameriavať na zavádzanie najmodernejších technológií ochrany údajov. V rovnakom duchu, ak OPP plánuje uplatňovať a používať TRT od externých poskytovateľov, musí zabezpečiť, napríklad prostredníctvom postupu verejného obstarávania, aby sa zaviedli len TRT založené na zásadách špecificky navrhnutej a štandardnej ochrany údajov[65]. Vyplýva z toho aj, že transparentnosť fungovania TRT nie je obmedzená tvrdeniami o obchodnom tajomstve alebo právach duševného vlastníctva.

---

[62] Viac informácií nájdete v dokumente WP248 rev.01 Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“.

[63] Pozri napríklad: ISO/IEC 24745 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia – ochrana biometrických informácií.

[64] Pozri odôvodnenie 53 LED.

[65] Ďalšie informácie nájdete v Usmerneniach EDPB k špecificky navrhnutej a štandardnej ochrane osobných údajov https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_sk.pdf.

#### *3.2.5.5 Článok 25 Logovanie*

101. V LED sa stanovujú rôzne metódy preukazovania zákonnosti spracúvania zo strany prevádzkovateľa alebo sprostredkovateľa a zabezpečenia integrity a bezpečnosti údajov. V tejto súvislosti sú systémové logy veľmi užitočným nástrojom a významnou zárukou overenia zákonnosti spracúvania, a to interne (t. j. vlastné monitorovanie), ako aj prostredníctvom externých dozorných orgánov, ako sú orgány na ochranu údajov. Podľa článku 25 LED by sa v automatizovaných systémoch spracúvania mali uchovávať logy aspoň o týchto spracovateľských operáciách: získavanie, zmena, prehliadanie, poskytovanie vrátane prenosov, kombinovanie a vymazanie. Okrem toho by z logov o prehliadaní a poskytovaní malo byť možné určiť dôvody, dátum a čas takýchto operácií, a pokiaľ možno aj identifikačné údaje osoby, ktorá tieto osobné údaje prehliadala alebo ich poskytovala, ako aj totožnosť príjemcov takýchto osobných údajov Okrem toho sa v súvislosti so systémami rozpoznávania tvárí odporúča logovanie týchto dodatočných spracovateľských operácií (čiastočne nad rámec článku 25 LED):

- Zmeny referenčnej databázy (pridanie, vymazanie alebo aktualizácia). Log by mal uchovávať kópiu príslušnej (pridaného, vymazaného alebo aktualizovaného) snímky, ak nie je inak možné overiť zákonnosť alebo výsledok spracovateľských operácií.

- Pokusy o identifikáciu alebo overenie vrátane výsledku a skóre spoľahlivosti. Mala by sa striktne uplatňovať zásada minimalizácie, aby sa v záznamoch uchovával len identifikátor snímky z referenčnej databázy namiesto ukladania referenčnej snímky. Malo by sa zabrániť logovaniu vstupných biometrických údajov, pokiaľ to nie je nevyhnutné (napr. len v prípadoch zhody)

- Identifikátor používateľa, ktorý požiadal o pokus o identifikáciu alebo overenie.

- Všetky osobné údaje uložené v logoch systémov podliehajú prísnym obmedzeniam účelu (napr. audity) a nemali by sa používať na iné účely (napr. aby nebolo možné naďalej vykonávať rozpoznávanie/overovanie na základe snímky, ktorá bol vymazaná z referenčných databáz). Na zabezpečenie integrity logov by sa mali uplatňovať bezpečnostné opatrenia, pričom sa odporúčajú automatické monitorovacie systémy na zisťovanie zneužitia protokolov. Pokiaľ ide o logy referenčných databáz, bezpečnostné opatrenia by pri ukladaní snímok tváre mali byť rovnocenné s referenčnou databázou. Takisto by sa mali zaviesť automatické postupy na zabezpečenie presadzovania doby uchovávania údajov v prípade logov.

#### *3.2.5.6 Článok 4 ods. 4 Zodpovednosť*

102. Prevádzkovateľ musí byť schopný preukázať súlad spracúvania so zásadami článku 4 ods. 1 až 3, pozri článok 4 ods. 4 LED. V tejto súvislosti má zásadný význam systematická a aktuálna dokumentácia systému (vrátane aktualizácií, modernizácie a trénovania algoritmu), technické a organizačné opatrenia (vrátane monitorovania výkonnosti systému a potenciálneho ľudského zásahu) a spracúvanie osobných údajov. Pri preukazovaní zákonnosti spracúvania je mimoriadne dôležitým prvkom logovanie podľa článku 25 LED (pozri oddiel 3.2.5.5). Zásada zodpovednosti sa nevzťahuje len na systém a spracúvanie, ale aj na dokumentáciu procesných záruk, ako sú posúdenia nevyhnutnosti a primeranosti, posúdenia vplyvu na ochranu údajov, ako aj interné konzultácie (napr. schválenie projektu zo strany vedenia alebo interné rozhodnutia o hodnotách skóre spoľahlivosti) a externé konzultácie (napr. s orgánom pre ochranu osobných údajov). Príloha II v tejto súvislosti obsahuje viacero prvkov.

#### *3.2.5.7 Článok 47 Účinný dohľad*

103. Účinný dohľad zo strany príslušných orgánov na ochranu údajov je jednou z najdôležitejších záruk základných práv a slobôd fyzických osôb, ktorých sa týka používanie TRT. Poskytnutie potrebných ľudských, technických a finančných zdrojov, priestorov a infraštruktúry každému orgánu na ochranu

údajov je zároveň predpokladom účinného plnenia ich úloh a výkonu ich právomocí[66]. Ešte dôležitejšie ako počet dostupných pracovníkov sú zručnosti odborníkov, ktorí by sa mali zaoberať veľmi širokým spektrom otázok - od vyšetrovania trestných činov a policajnej spolupráce až po analýzu veľkých dát a umelú inteligenciu. Členské štáty by preto mali zabezpečiť, aby zdroje dozorných orgánov boli primerané a dostatočné na to, aby mohli plniť svoj mandát na ochranu práv dotknutých osôb, a mali by pozorne sledovať akýkoľvek vývoj v tejto oblasti.[67]

# 4 ZÁVER

104. Používanie technológií rozpoznávania tváre je neoddeliteľne spojené so spracúvaním značných objemov osobných údajov vrátane osobitných kategórií údajov. Tvár a všeobecne biometrické údaje sú trvalo a neodvolateľne spojené s identitou osoby. Používanie rozpoznávania tváre má preto priamy alebo nepriamy vplyv na viaceré základné práva a slobody zakotvené v Charte základných práv EÚ, a môže ísť nad rámec ochrany súkromia a údajov, ako je ľudská dôstojnosť, sloboda pohybu, sloboda zhromažďovania a iné. Toto je obzvlášť dôležité v oblasti presadzovania práva a trestného súdnictva.

105. EDPB chápe potrebu orgánov presadzovania práva využívať najlepšie možné nástroje na rýchlu identifikáciu páchateľov teroristických činov a iných závažných trestných činov. Takéto nástroje by sa však mali používať v prísnom súlade s uplatniteľným právnym rámcom a len v prípadoch, keď spĺňajú požiadavky nevyhnutnosti a primeranosti, ako sa stanovuje v článku 52 ods. 1 Charty. Okrem toho, aj keď moderné technológie môžu byť súčasťou riešenia, v žiadnom prípade nejde o žiadne „zázračné riešenie“.

106. Existujú určité prípady použitia technológií rozpoznávania tváre, ktoré predstavujú neprijateľne vysoké riziko pre jednotlivcov a spoločnosť (tzv. červené čiary (red lines)). Z týchto dôvodov EDPB a EDPS vyzvali na ich všeobecný zákaz[68].

107. Najmä diaľková biometrická identifikácia jednotlivcov vo verejne prístupných priestoroch predstavuje vysoké riziko narušenia súkromného života jednotlivcov a nemá miesto v demokratickej spoločnosti, keďže vo svojej povahe zahŕňa hromadné sledovanie. V rovnakom duchu považuje EDPB systémy rozpoznávania tváre podporované umelou inteligenciou, ktoré kategorizujú osoby na základe ich biometrických údajov do skupín podľa etnického pôvodu, pohlavia, ako aj politickej alebo sexuálnej orientácie, za nezlučiteľné s Chartou. Okrem toho je EDPB presvedčený, že používanie technológií rozpoznávania tváre alebo podobných technológií na odvodzovanie emócií fyzickej osoby je absolútne nežiaduce a malo by byť zakázané, prípadne až na niekoľko riadne odôvodnených výnimiek. Okrem toho sa EDPB domnieva, že spracúvanie osobných údajov v kontexte presadzovania práva, ktoré by sa opieralo o databázu naplnenú zhromažďovaním osobných údajov v masovom rozsahu a nediferencovaným spôsobom, napr. extrahovaním (scraping) fotografií a obrázkov tváre dostupných online, najmä tých, ktoré sú dostupné prostredníctvom sociálnych sietí, by ako také nespĺňalo požiadavku úplnej nevyhnutnosti stanovenú v práve Únie.

[66] Pozri oznámenie Komisie s názvom Prvá správa o uplatňovaní a fungovaní smernice (EÚ) 2016/680 o ochrane údajov v oblasti presadzovania práva (LED), COM(2022) 364 final, bod 3.4.1.
[67] Pozri príspevok EDPB k hodnoteniu Európskej komisie smernice o presadzovaní práva v oblasti ochrany údajov (LED) podľa článku 62, bod 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf
[68] Pozri Spoločné stanovisko EDPB a EDPS 5/2021 k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_sk.pdf

# 5 PRÍLOHY

Príloha I: Pomocné predlohy

Príloha II: Praktické usmernenia pre riadenie projektov TRT v OPP

Príloha III: Praktické príklady

# PRÍLOHA I - PREDLOHA NA OPIS SCENÁROV

**(S informačnými rámčekmi pre aspekty riešené v rámci scenára)**

**Opis spracúvania:**

- Opis spracúvania, kontext (vzťah k trestnej činnosti), účel

**Zdroj informácií:**

- Typy dotknutých osôb: ☐ všetci občania ☐ odsúdené osoby ☐ podozrivé osoby
  ☐ deti ☐ iné zraniteľné dotknuté osoby
- Zdroj snímky: ☐ verejne prístupné priestory ☐ internet
  ☐ súkromný subjekt ☐ iné fyzické osoby ☐ iné .....
- Súvislosť s trestnou činnosťou: ☐ priama časová ☐ nepriama časová
  ☐ priama zemepisná ☐ nepriama zemepisná
  ☐ nie je potrebná
- Spôsob zachytávania informácií: ☐ na diaľku ☐ v kabíne alebo v kontrolovanom prostredí
- Kontext – vplyv na iné základné práva:
  ☐ Nie
  Áno, konkrétne☐ sloboda zhromažďovania
  ☐ Sloboda prejavu
  ☐ rôzne:.....
- Možnosti ďalších zdrojov informácií o dotknutej osobe:
  ☐ doklad totožnosti ☐ používanie verejného telefónu ☐ evidenčné číslo vozidla
  ☐ iné .....

**Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):**

- Špecifickosť: ☐ databázy na všeobecné účely ☐ špecifické databázy týkajúce sa oblasti trestnej činnosti
- Opis toho, ako boli tieto referenčné databázy naplnené (a právny základ)
- Zmena účelu databázy (napr. primárnym cieľom bola bezpečnosť súkromného majetku):
  ☐ ÁNO
  ☐ NIE

**Algoritmus:**

- Typ spracúvania: ☐ overenie jedna k jednej (autentifikácia) ☐ identifikácia jedna k mnohým
- Zváženie presnosti
- Technické záruky

**Výsledok:**

- Vplyv ☐ priamy (napr. dotknutá osoba môže byť zatknutá, vypočúvaná, diskriminačné správanie)

☐ nepriamy (použitie na štatistické modely, žiadne závažné právne kroky proti dotknutým osobám)

- Automatizované rozhodovanie: ☐ ÁNO ☐ NIE
- Dĺžka uchovávania

**Právna analýza:**

- Analýza nevyhnutnosti a primeranosti – účel/závažnosť trestnej činnosti/počet osôb, ktoré nie sú zapojené, ale sú ovplyvnené spracúvaním
- Typ predbežných informácií pre dotknutú osobu: ☐ Pri vstupe do konkrétnej oblasti
  ☐ Všeobecne na webovom sídle OPP
  ☐ Na webovom sídle OPP pre konkrétne spracúvanie
  ☐ Iné .....
- Uplatniteľný právny rámec :
  ☐ LED v prevažnej miere odkopírovaná do vnútroštátneho práva
  ☐ Všeobecné vnútroštátne právne predpisy o používaní biometrických údajov zo strany OPP
  ☐ Osobitné vnútroštátne právne predpisy pre toto spracúvanie (rozpoznávanie tvárí) pre daný príslušný orgán
  ☐ Osobitné vnútroštátne právne predpisy pre toto spracúvanie (automatizované rozhodovanie)

**Záver:**

Všeobecné úvahy o tom, či je opísané spracúvanie pravdepodobne zlučiteľné s právom EÚ (a niektoré náznaky právnych predpokladov)

# PRÍLOHA II - PRAKTICKÉ USMERNENIA PRE RIADENIE PROJEKTOV TRT V OPP

Táto príloha obsahuje niekoľko ďalších praktických usmernení pre orgány presadzovania práva (ďalej len „OPP“), ktoré plánujú začať projekt zahŕňajúci technológiu rozpoznávania tváre (ďalej len „TRT“). Poskytuje viac informácií o organizačných a technických opatreniach, ktoré treba zvážiť počas zavádzania projektu, a nemali by sa považovať za vyčerpávajúci zoznam krokov/opatrení, ktoré treba prijať. Mala by sa chápať v spojení s usmerneniami EDPB 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení[69] a všetkými nariadeniami EÚ/EHP a usmerneniami EDPB týkajúcimi sa využívania umelej inteligencie.

Táto príloha obsahuje usmernenia založené na predpoklade, že OPP budú TRT obstarávať (ako hotové produkty). Ak OPP plánuje vyvíjať (ďalej trénovať) TRT, potom sa uplatňujú ďalšie požiadavky na výber potrebných súborov údajov na trénovanie, validáciu a testovanie, ktoré sa majú použiť počas vývoja, a na roly/opatrenia pre vývojové prostredie. Podobne aj hotový výrobok si môže vyžadovať ďalšie úpravy na zamýšľané použitie, pričom v takom prípade by sa mali splniť uvedené požiadavky na výber súborov údajov na testovanie, validáciu a tréning.

Príslušnosť k tomu istému OPP sama o sebe neposkytuje úplný prístup k biometrickým údajom. Tak ako pri iných kategóriách osobných údajov, biometrické údaje získané na určitý účel presadzovania práva podľa osobitného právneho základu sa nemôžu použiť bez riadneho právneho základu na iný účel presadzovania práva [článok 4 ods. 2 smernice (EÚ) 2016/680 (LED)]. Vývoj/tréning nástroja TRT sa takisto považuje za iný účel a malo by sa posúdiť, či je spracúvanie biometrických údajov na meranie výkonnosti/trénovanie technológie na to, aby sa zabránilo vplyvu na dotknuté osoby v dôsledku nízkej výkonnosti, nevyhnutné a primerané vzhľadom na pôvodný účel spracúvania.

## 1. ÚLOHY A ZODPOVEDNOSTI

Ak OPP využíva TRT na plnenie svojich úloh, ktoré patria do rozsahu pôsobnosti LED (prevencia, vyšetrovanie, odhaľovanie alebo stíhanie trestných činov atď. podľa článku 3 LED), môže sa považovať za prevádzkovateľa TRT. OPP sa však skladajú z viacerých útvarov/oddelení, ktoré môžu byť do tohto spracúvania zapojené buď definovaním procesu uplatňovania TRT, alebo jeho uplatňovaním v praxi. Vzhľadom na špecifiká tejto technológie môže byť potrebné zapojiť rôzne útvary buď na podporu meraní jej výkonnosti, alebo na jej ďalší tréning.

V rámci projektu, ktorý zahŕňa nástroj TRT, existuje niekoľko zainteresovaných strán[70] v rámci OPP, ktoré možno budú musieť byť zapojené:

- Vrcholový manažment – schválenie projektu po zvážení rizík a potenciálnych prínosov.

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

[70] Nasledujúce roly sú orientačné pre rôzne zainteresované strany a ich zodpovedností v rámci projektu TRT. Hoci znenie textu použité na opis úloh v tejto prílohe nie je konkrétny, každý OPP musí vymedziť a prideliť podobné roly podľa svojej organizácie. Môže sa stať, že útvaru bude prináležať viac ako jedna rola, napríklad vlastník procesu a správca referenčnej databázy alebo vlastník procesu a oddelenie IT umelej inteligencie a/alebo dátovej vedy (v prípade, že oddelenie vlastníka procesu má všetky potrebné technické znalosti).

- Zodpovedná osoba (DPO) a/alebo právne oddelenie OPP – pomoc pri posudzovaní zákonnosti realizácie určitého projektu TRT; pomoc pri vykonávaní posúdenia vplyvu na ochranu údajov; zabezpečovať dodržiavanie a uplatňovanie práv dotknutých osôb.
- Vlastník procesu – konajúci ako osobitný subjekt v rámci príslušného OPP pri vývoji projektu, rozhodovaní o podrobnostiach projektu TRT vrátane požiadaviek na výkonnosť systému; rozhodovaní o vhodnej metrike spravodlivosti; stanovovaní skóre spoľahlivosti[71]; stanovovaní prijateľných prahov zaujatosti; identifikácii potenciálnych rizík, ktoré projekt TRT predstavuje pre práva a slobody jednotlivcov (konzultáciou aj so zodpovednou osobou a oddelením IT umelej inteligencie a/alebo dátovej vedy (pozri ďalej)) a ich predkladaní vrcholovému manažmentu. Pred tým, ako sa rozhodne o podrobnostiach projektu TRT, vlastník procesu bude konzultovať aj so správcom referenčnej databázy, aby pochopil účel použitia referenčnej databázy, ale aj jej technické podrobnosti. V prípade ďalšieho tréningu [re-training] obstaranej TRT bude vlastník procesu zodpovedný aj za výber súboru údajov na tréning. Ako subjekt poverený vypracovaním a rozhodovaním o podrobnostiach projektu je za vykonávanie posúdenia vplyvu na ochranu údajov zodpovedný vlastník procesu.
- IT oddelenie pre umelú inteligenciu a/alebo pre dátovú vedu – pomoc pri vykonávaní posúdenia vplyvu na ochranu údajov; vysvetlenie dostupných metrík na meranie výkonnosti systému, spravodlivosti[72] a potenciálnej zaujatosti; zavádzanie technológie a technických záruk s cieľom zabrániť neoprávnenému prístupu k získaným údajom, zabraňovanie kybernetickým útokom atď. V prípade ďalšieho tréningu obstaranej TRT, IT oddelenie pre umelú inteligenciu alebo pre dátovú vedu vytrénuje systém na základe tréningového súboru údajov, ktorý poskytol vlastník procesu. Toto oddelenie bude zodpovedné aj za zavedenie opatrení na zmiernenie rizík, ktoré spoločne identifikovali vlastníci procesov (napr. riziká špecifické pre umelú inteligenciu, ako sú napríklad inferenčné útoky na model).
- Koncoví používatelia (napríklad policajti v teréne alebo v kriminalistických laboratóriách) – vykonanie porovnania s databázou; kritické preskúmanie výsledkov s prihliadnutím na predchádzajúce dôkazy a poskytnutie spätnej väzby vlastníkovi procesu pokiaľ ide o falošne pozitívne výsledky a náznaky možnej diskriminácie.
- Správca referenčnej databázy – osobitný útvar v rámci príslušného OPP zodpovedný za zhromažďovanie údajov referenčnej databázy a jej správu, t. j. databázy, s ktorou sa porovnávajú snímky, vrátane vymazávania snímok tváre po uplynutí stanovenej doby uchovávania. Takáto databáza môže byť vytvorená špeciálne pre plánovaný projekt TRT alebo môže existovať už predtým na zlučiteľné účely. Správca referenčnej databázy je zodpovedný za definovanie toho, kedy a za akých okolností sa môžu snímky tváre uchovávať, ako aj za stanovenie požiadaviek na uchovávanie údajov (podľa časových alebo iných kritérií).

Keďže väčšina prípadov zavádzania a používania TRT predstavuje vysoké riziko pre práva a slobody dotknutých osôb, v rámci predchádzajúcej konzultácie požadovanej podľa článku 28 LED by mal byť zapojený aj dozorný orgán pre ochranu údajov.

[71] Skóre spoľahlivosti je úroveň dôveryhodnosti predpovede (zhody) vo forme pravdepodobnosti. Napr. pri porovnaní dvoch vzorov je 90 % pravdepodobnosť, že patria tej istej osobe. Skóre spoľahlivosti je odlišné od výkonnosti TRT, ale ovplyvňuje výkonnosť. Čím vyšší je prah spoľahlivosti, tým menej falošne pozitívnych výsledkov a viac falošných negatívnych výsledkov sa vyskytuje vo výsledkoch TRT.

[72] Spravodlivosť možno definovať ako absenciu nespravodlivej, nezákonnej diskriminácie, napríklad rodovej alebo rasovej zaujatosti.

# 2. ZAČIATOK/PRED OBSTARANÍM SYSTÉMU TRT

Vlastník procesu v rámci OPP by mal najskôr jasne chápať proces (procesy) využívania TRT (prípad/prípady použitia) a mal by zabezpečiť právny základ na odôvodnenie zamýšľaného použitia. Na základe uvedeného je potrebné urobiť:

- Formálny opis prípadu použitia. Je potrebné opísať problém, ktorý sa má vyriešiť, a spôsob, akým TRT poskytne riešenie, ako aj prehľad o procese (úlohe), v rámci ktorého sa bude uplatňovať. V tejto súvislosti by mali OPP zdokumentovať aspoň[73]:
  - Kategórie osobných údajov zaznamenaných v procese
  - Ciele a konkrétne účely, na ktoré sa bude TRT používať, vrátane možných dôsledkov pre dotknutú osobu v prípade zhody.
  - Kedy a ako sa budú získavať snímky tváre (vrátane informácií o kontexte tohto získavania, napr. pri letiskovej bráne, videá z bezpečnostných kamier pred obchodom, v ktorom bol spáchaný trestný čin atď., a kategórií dotknutých osôb, ktorých biometrické údaje sa budú spracúvať).
  - Databáza, s ktorou sa budú snímky porovnávať (referenčná databáza), ako aj informácie o tom, ako bola vytvorená, o jej veľkosti a kvalite biometrických údajov, ktoré obsahuje.
  - Aktéri OPP, ktorí budú oprávnení používať systém TRT a konať na jeho základe v kontexte presadzovania práva (ich profily a prístupové práva musí definovať vlastník procesu).
  - Predpokladaná doba uchovávania vstupných údajov alebo okamih, ktorý určí koniec tejto doby (napríklad uzatvorenie alebo ukončenie trestného konania v súlade s vnútroštátnym procesným právom, pre ktoré boli údaje pôvodne získané), ako aj všetky následné opatrenia (vymazanie týchto údajov, anonymizácia a použitie na štatistické alebo výskumné účely atď.).
  - Vykonávanie logovania a prístupnosť vedených logov a záznamov.
  - Metriky výkonnosti (napr. správnosť, presnosť, odozva, skóre F1) a ich minimálne prijateľné prahové hodnoty.[74]
  - Odhad, na koľko ľudí sa bude TRT vzťahovať v akom období/pri akej príležitosti.
- Vykonanie posúdenia nevyhnutnosti a primeranosti[75]. Skutočnosť, že táto technológia existuje, by nemala byť impulzom pre jej využitie. Vlastník procesu musí najprv posúdiť, či existuje primeraný právny základ pre plánované spracúvanie. Na tento účel je potrebné konzultovať so zodpovednou osobou (DPO) a právnym oddelením. Impulzom pre zavádzanie TRT by malo byť to, že ide o nevyhnutné a primerané riešenie konkrétne definovaného problému OPP. Malo by sa to posúdiť podľa účelu/závažnosti trestného činu/počtu osôb, ktoré nie sú zapojené, ale sú ovplyvnené systémom TRT. Pri posudzovaní zákonnosti by sa mali zvážiť aspoň tieto aspekty: LED[76], všeobecné

[73] V prílohe I sa uvádza zoznam prvkov, ktoré prevádzkovateľovi pomôžu opísať prípad použitia TRT.

[74] Existujú rôzne metriky na hodnotenie výkonnosti systému TRT. Každá metrika poskytuje iný pohľad na výsledky systému a jej úspešnosť pri poskytovaní adekvátneho obrazu o tom, či systém TRT funguje dobre alebo nie, závisí od prípadu použitia TRT. Ak sa dôraz kladie na dosiahnutie vysokých percentuálnych podielov správneho priradenia tváre, mohli by sa použiť ukazovatele ako je presnosť a odozva. Tieto metriky však nemerajú ako dobre TRT zvláda negatívne príklady (koľko z nich systém priradí nesprávne). Vlastník procesu s podporou IT oddelenia pre umelú inteligenciu a pre dátovú vedu by mal byť schopný stanoviť výkonnostné požiadavky a vyjadriť ich pomocou najvhodnejšej metriky podľa prípadu použitia TRT.

[75] Ďalšie kroky na zabezpečenie nevyhnutnosti sa môžu zvážiť v súvislosti s prispôsobením a používaním systému, takže opis prípadu použitia sa môže mierne zmeniť aj počas posudzovania nevyhnutnosti a primeranosti.

[76] Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií.

nariadenie o ochrane údajov[77] [78], akýkoľvek existujúci právny rámec týkajúci sa umelej inteligencie[79], a všetky sprievodné usmernenia poskytnuté dozornými orgánmi na ochranu údajov (napríklad usmernenia EDPB 3/2019 k spracúvaniu osobných údajov prostredníctvom kamerových zariadení[80]). Tieto akty právnych predpisov EÚ by mali byť vždy potvrdené uplatniteľnými vnútroštátnymi požiadavkami, najmä v oblasti trestného procesného práva. Pri posúdení primeranosti by sa mali identifikovať základné práva dotknutých osôb, ktoré môžu byť dotknuté (nad rámec ochrany súkromia a údajov). Takisto by sa mali opísať a zvážiť všetky obmedzenia (alebo chýbajúce obmedzenia) uložené v prípade použitia systému TRT. Napríklad, či bude systém fungovať nepretržite alebo dočasne a či bude obmedzený na určitú zemepisnú oblasť.

- Vykonanie posúdenia vplyvu na ochranu údajov[81]. Posúdenie vplyvu na ochranu údajov by sa malo vykonávať, keďže zavedenie TRT v oblasti presadzovania práva môže viesť k vysokému riziku pre práva a slobody jednotlivcov[82]. Posúdenie vplyvu na ochranu údajov by malo obsahovať najmä: všeobecný opis plánovaných spracovateľských operácií[83], hodnotenie rizík pre práva a slobody dotknutých osôb[84], plánované opatrenia na riešenie týchto rizík, záruky, bezpečnostné opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov a na preukázanie súladu. Posúdenie vplyvu na ochranu údajov je prebiehajúci proces, takže akékoľvek nové prvky spracúvania by sa mali doplniť a posúdenie rizika by sa malo aktualizovať v každej fáze projektu.
- Získanie súhlasu vrcholového manažmentu vysvetlením rizík pre práva a slobody dotknutých osôb (vyplývajúcich z prípadu použitia a technológie) a príslušných plánov riešenia týchto rizík.

# 3. POČAS OBSTARÁVANIA A PRED ZAVEDENÍM TRT

- Rozhodnutie o kritériách pre výber TRT (algoritmu). Vlastník procesu by mal s pomocou IT oddelenia pre umelú inteligenciu a/alebo dátovú vedu rozhodnúť o kritériách výberu algoritmu. V praxi by to zahŕňalo metriky spravodlivosti a výkonu, o ktorých sa rozhodlo v opise prípadu použitia. Takéto kritériá by mali zahŕňať aj informácie týkajúce sa údajov, na ktorých bol

[77] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov.

[78] V prípadoch, že by vedecký projekt zameraný na výskum používania TRT potreboval spracúvať osobné údaje, ale takéto spracúvanie by nespadalo pod článok 4 ods. 3 LED, by sa vo všeobecnosti uplatňovalo všeobecné nariadenie o ochrane údajov (článok 9 ods. 2 LED). V prípade pilotných projektov, po ktorých by nasledovali operácie presadzovania práva, by sa ale uplatňovala LED.

[79] Existuje napríklad návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, KTORÝM SA STANOVUJÚ HARMONIZOVANÉ PRAVIDLÁ V OBLASTI UMELEJ INTELIGENCIE (AKT O UMELEJ INTELIGENCII) A MENIA NIEKTORÉ LEGISLATÍVNE AKTY ÚNIE, ktorý však zatiaľ nie je prijatý ako nariadenie.

[80] https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_sk.pdf.

[81] Ďalšie usmernenia k posúdeniam vplyvu na ochranu údajov možno nájsť v: Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku, WP 248 rev.01, dostupné na : https://ec.europa.eu/newsroom/article29/items/611236 a súbor nástrojov EDPS pre zodpovednosť v teréne, časť II, dostupné na: https://edps.europa.eu/node/4582_en

[82] TRT môže v závislosti od prípadu použitia spadať pod tieto kritériá, ktoré vedú k spracúvaniu s vysokým rizikom (z Usmernení týkajúcich sa DPIA, WP 248 rev.01): Systematické monitorovanie, spracúvanie údajov vo veľkom rozsahu, porovnávanie alebo kombinovanie súborov údajov, inovatívne využívanie alebo uplatňovanie nových technologických alebo organizačných riešení.

[83] Opis spracúvania, ako aj posúdenie nevyhnutnosti a primeranosti, ako už boli opísané v uvedených krokoch, sú okrem posúdenia rizika aj súčasťou posúdenia vplyvu na ochranu údajov. V prípade potreby sa v posúdení vplyvu na ochranu údajov uvedie podrobnejší opis tokov osobných údajov.

[84] Analýza rizík pre dotknuté osoby by mala zahŕňať riziká súvisiace s miestom porovnávania snímok tváre (na mieste/vzdialené), riziká súvisiace so sprostredkovateľmi/ďalšími sprostredkovateľmi, ako aj riziká špecifické pre strojové učenie, ak sa uplatňuje (napr. otrávenie údajov, odporujúce si príklady).

algoritmus trénovaný. Tréningový, testovací a validačný súbor musí v dostatočnej miere obsahovať vzorky všetkých charakteristík dotknutých osôb, pri ktorých sa má používať TRT (zvážiť napríklad vek, pohlavie a rasu), aby sa znížila zaujatosť. Poskytovateľ TRT by mal poskytnúť informácie a metriky týkajúce sa tréningových, testovacích a validačných súborov údajov TRT a opísať opatrenia prijaté na meranie a zmiernenie potenciálnej nezákonnej diskriminácie a zaujatosti. Vlastník procesu musí, ak je to možné, skontrolovať, či existuje právny základ pre poskytovateľa na používanie tohto súboru údajov na účely trénovania algoritmov (na základe informácií, ktoré poskytovateľ sprístupní). Vlastník procesu by mal tiež zabezpečiť, aby poskytovateľ TRT uplatňoval bezpečnostné normy týkajúce sa biometrických údajov, ako je napríklad norma ISO/IEC 24745, ktorá poskytuje usmernenia na ochranu biometrických informácií v rámci rôznych požiadaviek na dôvernosť, integritu a obnoviteľnosť/odvolateľnosť počas uchovávania a prenosu a požiadavky a usmernenia na bezpečnú správu a spracúvanie biometrických informácií v súlade s ochranou súkromia.

- Ďalšie trénovanie algoritmu (v prípade potreby), Vlastník procesu by mal zabezpečiť, aby doladenie systému TRT na dosiahnutie vyššej presnosti pred jeho použitím bolo takisto súčasťou obstarávaných služieb. V prípade, že na splnenie metriky presnosti je potrebný ďalší tréning nadobudnutého systému TRT, vlastník procesu musí okrem prijatia rozhodnutia o ďalšom tréningu rozhodnúť s pomocou IT oddelenia pre umelú inteligenciu a/alebo dátovú vedu o primeranom, reprezentatívnom súbore údajov, ktorý sa má použiť, a skontrolovať zákonnosť tohto použitia údajov.
- Nastavenie vhodných záruk na riešení rizík súvisiacich s bezpečnosťou, zaujatosťou a nízkou výkonnosťou. Patrí sem aj zavedenie postupu na monitorovanie TRT po začatí jej používania (logovanie a spätná väzba v záujme správnosti a spravodlivosti výsledkov). Okrem toho je potrebné zabezpečiť, aby sa identifikovali, merali a zmierňovali riziká, ktoré sú špecifické pre niektoré systémy strojového učenia a systémy TRT (napr. odtajnenie údajov, odporujúce si príklady, inverzia modelu, inferencia bielej schránky). Vlastník procesu by mal okrem toho stanoviť primerané záruky, aby sa zabezpečilo, že sa budú dodržiavať požiadavky na uchovávanie biometrických údajov zahrnutých do súboru údajov určených na ďalšie trénovanie.
- Zdokumentovanie systému TRT. Malo by obsahovať všeobecný opis systému TRT, podrobný opis prvkov systému TRT a procesu jeho zavedenia, podrobné informácie o monitorovaní, fungovaní a kontrole systému TRT a podrobný opis jeho rizík a opatrení na ich zmiernenie. Prvky zahrnuté v tejto dokumentácii budú zahŕňať hlavné prvky opisu systému TRT z predchádzajúcich fáz (pozri vyššie), ktoré však budú rozšírené o informácie týkajúce sa monitorovania výkonnosti a uplatňovania zmien v systéme vrátane akýchkoľvek aktualizácií verzií a/alebo ďalšieho tréningu.
- Vytvorenie používateľských príručiek s vysvetlením technológie a prípadov použitia. V nich musia byť jasne vysvetlené všetky scenáre a predpoklady, na základe ktorých sa bude TRT používať.
- Vyškolenie koncových používateľov o tom, ako používať technológiu. Takéto školenia musia vysvetliť schopnosti a obmedzenia technológie, aby používatelia pochopili okolnosti, za ktorých je potrebné ju uplatňovať, a prípady, v ktorých môže byť nepresná. Takéto školenia pomôžu aj pri zmierňovaní rizík súvisiacich s nekontrolovaním/kritizovaním výsledkov algoritmu.
- Konzultácia s dozorným orgánom pre ochranu údajov podľa článku 28 ods. 1 písm. b) LED. Poskytnutie informácií podľa článku 13 LED s cieľom informovať dotknuté osoby o spracúvaní a ich právach. Tieto informácie sa musia adresovať dotknutým osobám vhodnou formou, aby boli schopné porozumieť spracúvaniu a musia sa im vysvetliť základné prvky technológie vrátane miery správnosti, tréningových súborov údajov a opatrení prijatých na zabránenie diskriminácie a nízkej správnosti algoritmu.

# 4. ODPORÚČANIA PO ZAVEDENÍ TRT

- Zabezpečenie ľudského zásahu a dohľadu nad výsledkami. Nikdy neprijmite žiadne opatrenie týkajúce sa jednotlivca výlučne na základe výsledku TRT (znamenalo by to porušenie článku 11 o automatizovanom individuálnom rozhodovaní LED, čo má právne alebo iné podobné účinky na dotknutú osobu). Zabezpečte, aby príslušník OPP preskúmal výsledky TRT. Zabezpečte tiež, aby sa používatelia OPP vyhli nadmernému dôverovaniu automatizácii tým, že budú skúmať protichodné informácie a kriticky spochybňovať výsledky technológie. Na tento účel je dôležitá sústavná odborná príprava a zvyšovanie informovanosti koncových používateľov, vrcholový manažment by však mal zabezpečiť primerané ľudské zdroje na vykonávanie účinného dohľadu. To znamená poskytnúť každému aktérovi dostatok času na kritické spochybnenie výsledkov technológie. Zaznamenať, zmerať a posúdiť, do akej miery ľudský dohľad mení pôvodné rozhodnutie TRT.
- Monitorovanie a riešenie odchýlky modelu TRT (zhoršovanie výkonnosti) po uvedení modelu do prevádzky.
- Zavedenie postupu pravidelného prehodnocovania rizík a bezpečnostných opatrení a vždy, keď technológia alebo prípad použitia prejde akýmikoľvek zmenami.
- Dokumentovanie každej zmeny systému počas jeho životného cyklu (napr. aktualizácie, ďalšie trénovanie).
- Stanovenie postupu, ako aj súvisiace technické možnosti na riešenie žiadostí dotknutých osôb o prístup. Technická možnosť extrakcie údajov v prípade, že je potrebné ich poskytnúť dotknutým osobám, musí existovať pred podaním akejkoľvek žiadosti.
- Zabezpečenie toho, aby boli zavedené postupy pre prípady porušenia ochrany údajov [data breaches]. Ak dôjde k porušeniu ochrany osobných údajov vrátane biometrických údajov, riziká budú pravdepodobne vysoké. V tomto prípade by všetci zúčastnení používatelia mali byť informovaní o príslušných postupoch, ktoré sa majú dodržiavať, bezodkladne by mala byť informovaná zodpovedná osoba, a informované by mali byť aj dotknuté osoby.

# PRÍLOHA III - PRAKTICKÉ PRÍKLADY

Existuje mnoho rôznych praktických nastavení a účelov používania rozpoznávania tváre, napríklad v kontrolovanom prostredí, ako je napríklad pri prekračovaní hraníc, krížová kontrola s údajmi z policajných databáz alebo osobných údajov preukázateľne sprístupnených dotknutou osobou, priamy prenos z kamery (rozpoznanie tváre v reálnom čase) atď. V dôsledku toho sa riziká pre ochranu osobných údajov a iných základných práv a slobôd v jednotlivých prípadoch použitia výrazne líšia. S cieľom uľahčiť posúdenie nevyhnutnosti a primeranosti, ktoré by malo predchádzať rozhodnutiu o možnom nasadení rozpoznávania tváre, sa v súčasných usmerneniach uvádza neúplný zoznam možných aplikácií TRT v oblasti presadzovania práva.

Predložené a posudzované scenáre sú založené na **hypotetických** situáciách a ich cieľom je ilustrovať určité konkrétne použitia TRT a poskytnúť pomoc pri posudzovaní jednotlivých prípadov, ako aj stanoviť celkový rámec. Nesnažia sa byť vyčerpávajúce a nie sú nimi dotknuté žiadne prebiehajúce alebo budúce konania vedené vnútroštátnym dozorným orgánom, pokiaľ ide o navrhovanie, experimentovanie alebo zavádzanie technológií rozpoznávania tváre. Prezentácia týchto scenárov by mala slúžiť len na účely ilustrácie usmernení pre tvorcov politík, zákonodarcov a orgány presadzovania práva, ktoré sú už uvedené v tomto dokumente, pri navrhovaní a plánovaní zavádzania technológií rozpoznávania tváre s cieľom zabezpečiť úplný súlad s acquis EÚ v oblasti ochrany osobných údajov. V tejto súvislosti treba mať na pamäti, že aj v podobných situáciách použitia TRT môže prítomnosť alebo neprítomnosť určitých prvkov viesť k odlišnému výsledku posúdenia nevyhnutnosti a primeranosti.

## 1 SCENÁR 1

### 1.1. Popis

Automatizovaný systém hraničnej kontroly, ktorý umožňuje automatizovaný prechod cez hranice prostredníctvom autentifikácie biometrickej snímky [biometric image] uloženej v elektronickom cestovnom doklade občanov EÚ a iných cestujúcich prechádzajúcich cez hraničný priechod a zistenia, že cestujúci je oprávneným držiteľom dokladu.

Takéto overovanie/autentifikácia zahŕňa len individuálne rozpoznávanie tváre a vykonáva sa v kontrolovanom prostredí (napr. pri letiskových elektronických bránach). Biometrické údaje cestujúceho, ktorý prechádza cez hraničný priechod, sa zachytia, keď je výslovne vyzvaný, aby sa pozrel do kamery v elektronickej bráne, a porovnajú sa s údajmi z predloženého dokladu (cestovný pas, preukaz totožnosti atď.), ktorý sa vydáva podľa osobitných technických požiadaviek.

Hoci spracúvanie v takýchto prípadoch v zásade nepatrí do rozsahu pôsobnosti LED, výsledok overenia sa môže použiť aj pri porovnávaní (alfanumerických) údajov osoby s databázami orgánov presadzovania práva v rámci kontroly hraníc, a teda môže zahŕňať opatrenia s významným právnym účinkom pre dotknutú osobu, napr. zadržanie na základe zápisu v SIS. Za určitých okolností sa biometrické údaje môžu použiť aj na hľadanie zhody v databázach OPP (v takom prípade by sa v tomto kroku vykonala identifikácia jedna k jednej).

Výsledok spracúvania biometrických snímok má priamy vplyv na dotknutú osobu: iba v prípade úspešného overenia umožňuje prechod cez hraničný priechod. V prípade neúspešnej identifikácie musia príslušníci pohraničnej stráže vykonať druhú kontrolu, aby sa uistili, že dotknutá osoba je iná ako tá, ktorá je uvedená v doklade totožnosti.

V prípade identifikácie zápisu v SIS alebo vnútroštátneho záznamu musia príslušníci pohraničnej stráže vykonať druhé overenie a ďalšie potrebné kontroly a potom prijať všetky potrebné opatrenia, napr. zadržať osobu, informovať príslušné orgány.

Zdroj informácií:

- Typy dotknutých osôb: ☒ všetky fyzické osoby prekračujúce hranice
- Zdroj snímky: ☒ iné (doklad totožnosti)
- Spojenie s trestnou činnosťou :☒ nemusí byť
- Spôsob zachytávania informácií:☒ v kabíne alebo kontrolovanom prostredí
- Kontext - vplyv na iné základné práva: Áno, konkrétne: ☒ právo na voľný pohyb ☒ právo na azyl

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť: ☒ špecifické databázy týkajúce sa kontroly hraníc

Algoritmus:

- Typ overovania:☒ overenie jedna k jednej (autentifikácia)

Výsledok:

- Vplyv ☒ priamy (dotknutej osobe je povolený alebo zamietnutý vstup)
- Automatizované rozhodovanie: ☒ Áno

## 1.2. Uplatniteľný právny rámec

Od roku 2004 musia podľa nariadenia Rady (ES) č. 2252/2004[85] pasy a iné cestovné doklady vydávané členskými štátmi obsahovať biometrické snímky tváre [biometric facial image] uložené v elektronickom čipe začlenenom v doklade.

V Kódexe schengenských hraníc[86] sa stanovujú požiadavky na hraničné kontroly osôb na vonkajších hraniciach. V prípade občanov EÚ a iných osôb, ktoré požívajú právo na voľný pohyb v súlade s právom Únie, by minimálne kontroly mali pozostávať z overenia ich cestovných dokladov, v prípade potreby pomocou technických zariadení. Kódex schengenských hraníc bol následne zmenený nariadením (EÚ) 2017/2225[87], ktorým sa zaviedli, *okrem iného*, definície pojmov „elektronické brány“, „automatizovaný systém hraničnej kontroly“ a „samoobslužný systém“, ako aj možnosť spracúvania biometrických údajov na účely vykonávania hraničných kontrol.

Preto by sa dalo predpokladať, že existuje jasný a predvídateľný právny základ, ktorý by umožňoval túto formu spracúvania osobných údajov. Okrem toho je právny rámec prijatý na úrovni Únie a priamo sa uplatňuje na členské štáty.

## 1.3. Nevyhnutnosť a primeranosť – účel/závažnosť trestného činu

Overovanie totožnosti občanov EÚ pri automatizovanej kontrole hraníc pomocou ich biometrickej snímky je prvkom hraničných kontrol na vonkajších hraniciach EÚ. Preto priamo súvisí s bezpečnosťou hraníc a slúži cieľu všeobecného záujmu, ktorý uznáva Únia. Okrem toho brány automatizovanej kontroly hraníc pomáhajú urýchliť odbavovanie cestujúcich a znižujú riziko ľudských chýb. Navyše je rozsah, miera a intenzita rušenia v tomto scenári oveľa obmedzenejšia v porovnaní s inými formami

[85] Nariadenie Rady (ES) č. 2252/2004 z 13. decembra 2004 o normách pre bezpečnostné znaky a biometriu v pasoch a cestovných dokladoch vydávaných členskými štátmi.
[86] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/399 z 9. marca 2016, ktorým sa ustanovuje kódex Únie o pravidlách upravujúcich pohyb osôb cez hranice (Kódex schengenských hraníc)
[87] Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/2225 z 30. novembra 2017, ktorým sa mení nariadenie (EÚ) 2016/399, pokiaľ ide o používanie systému vstup/výstup.

rozpoznávania tváre. Spracúvanie biometrických údajov však vytvára pre dotknuté osoby dodatočné riziká, ktoré musí príslušný orgán zavádzajúci a prevádzkujúci TRT náležite riešiť a zmierňovať.

### 1.4. Záver

Overenie totožnosti občanov EÚ v kontexte automatizovanej kontroly hraníc je nevyhnutným a primeraným opatrením, pokiaľ sú zavedené primerané záruky, najmä uplatňovanie zásad obmedzenia účelu, kvality údajov, transparentnosti a vysokej úrovne bezpečnosti.

## 2 SCENÁR 2

### 2.1. Popis

Systém identifikácie obetí únosu dieťaťa stanovujú OPP. Poverený príslušník polície môže za prísne stanovených podmienok porovnať biometrické údaje dieťaťa, pri ktorom existuje podozrenie z únosu, s databázou obetí únosov detí, a to výlučne na účely identifikácie maloletých osôb, ktoré môžu zodpovedať opisu nezvestného dieťaťa, v súvislosti s ktorým sa začalo vyšetrovanie a bolo vydané upozornenie [alert].

Predmetným spracúvaním by bolo porovnanie tváre alebo snímky osoby, ktorá môže zodpovedať opisu nezvestného dieťaťa, so snímkami uloženými v databáze. Takéto spracúvanie by sa uskutočňovalo v osobitných prípadoch, a nie na systematickom základe.

Databáza, na základe ktorej sa porovnanie vykoná, je naplnená fotografiami nezvestných detí, v prípade ktorých bolo nahlásené podozrenie z únosu dieťaťa, ohrozenia jeho života alebo telesnej integrity, a v prípade ktorých bolo začaté trestné stíhanie na základe rozhodnutia súdneho orgánu, a v prípade ktorých bolo vydané upozornenie na únos dieťaťa. Údaje sa získavajú v rámci postupov stanovených príslušným OPP, t. j. príslušníci polície oprávnení vykonávať misie justičnej polície. Kategórie zaznamenávaných osobných údajov sú:

- totožnosť, prezývka, alias, príbuzenský vzťah, štátna príslušnosť, adresy, e-mailové adresy, telefónne čísla;
- dátum a miesto narodenia;
- informácie o rodičovstve;
- fotografia s technickými vlastnosťami umožňujúcimi použitie zariadenia na rozpoznávanie tváre a iné fotografie.

Výsledky porovnania musí preskúmať a overiť aj oprávnený pracovník s cieľom potvrdiť predchádzajúce dôkazy s výsledkom porovnania a vylúčiť akékoľvek možné falošné pozitívne výsledky.

Fotografie a osobné údaje detí sa môžu uchovávať len počas trvania upozornenia a musia sa vymazať okamžite po uzatvorení alebo skončení trestného konania v súlade s vnútroštátnymi postupmi, na základe ktorého boli vložené do databázy.

Zatiaľ čo doba uchovávania biometrických údajov v databáze môže byť stanovená na pomerne dlhé obdobie a vymedzená podľa vnútroštátneho práva, uplatňovanie práv dotknutých osôb, a najmä práva na opravu a vymazanie, poskytuje dodatočnú záruku na obmedzenie zásahov do práva na ochranu osobných údajov týchto dotknutých osôb.

| Zdroj informácií: |
|---|

- Typy dotknutých osôb: ☒ deti
- Zdroj snímky ☒ iný: nie je preddefinovaný, podozrivá obeť únosu dieťaťa
- Súvislosť s trestnou činnosťou ☒ nepriama časová ☒ nepriama geografická
- Spôsob zachytávania informácií: ☒ v kabíne alebo kontrolovanom prostredí
- Kontext: vplyv na iné základné práva ☒ Áno, konkrétne: ☒ rôzne

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť ☒ špecifická databáza

Algoritmus:

- Typ overenia: ☒ identifikácia jedna k mnohým

Výsledok:

- Vplyv ☒ priamy
- Automatizované rozhodovanie: ☒ NIE, povinné preskúmanie oprávneným pracovníkom

Právna analýza:

- Uplatniteľný právny rámec: ☒ osobitné vnútroštátne právne predpisy pre toto spracúvanie (rozpoznávanie tváre)

## 2.2. Uplatniteľný právny rámec

Vo vnútroštátnych právnych predpisoch sa stanovuje osobitný právny rámec, ktorým sa zriaďuje databáza a určujú sa účely spracúvania, ako aj kritériá na naplnenie databázy, prístup k nej a jej používanie. Legislatívne opatrenia potrebné na vykonávanie tiež stanovujú určenie doby uchovávania, ako aj odkaz na platné zásady integrity a dôvernosti. V legislatívnych opatreniach sa takisto stanovujú spôsoby poskytovania informácií dotknutej osobe a v tomto prípade nositeľovi (nositeľom) rodičovských práv a povinností, ako aj výkon práv dotknutej osoby a ich prípadné obmedzenie. Počas prípravy návrhu príslušného legislatívneho opatrenia bolo potrebné konzultovať s vnútroštátnym dozorným orgánom.

## 2.3. Nevyhnutnosť a primeranosť – účel/závažnosť trestnej činnosti/počet osôb, ktoré nie sú zapojené, ale sú ovplyvnené spracúvaním

*Podmienky a záruky spracúvania*

Porovnanie v rámci rozpoznávania tváre môže vykonať iba oprávnený pracovník ako poslednú možnosť, pokiaľ nie sú k dispozícii iné, menej rušivé prostriedky a ak je to úplne nevyhnutné napríklad v prípade pochybností o pravosti cestovného dokladu totožnosti maloletej osoby a/alebo po preskúmaní predchádzajúcich dôkazov a zhromaždených materiálov naznačujúcich možnú zhodu s opisom nezvestného dieťaťa, v prípade ktorého prebieha vyšetrovanie trestného činu.

Dodatočnú záruku poskytuje aj povinné preskúmanie a overenie porovnania v rámci rozpoznávania tváre oprávneným pracovníkom s cieľom potvrdiť predchádzajúce dôkazy s výsledkom porovnania a vylúčiť akékoľvek prípadné falošne pozitívne výsledky.

*Sledovaný cieľ*

Zriadenie databázy slúži dôležitým cieľom všeobecného verejného záujmu, najmä predchádzaniu, vyšetrovaniu, odhaľovaniu alebo stíhaniu trestných činov alebo výkonu trestných sankcií a ochrane práv a slobôd iných. Vytvorenie databázy a predpokladané spracúvanie podľa všetkého prispieva k identifikácii detí, ktoré sa stali obeťami únosu, a preto sa môže považovať za opatrenie vhodné na podporu oprávneného cieľa vyšetrovania a stíhania takýchto trestných činov.

*Účel a naplnenie databázy*

Účely spracúvania sú jasne vymedzené zákonom a databáza sa používa len na účely identifikácie nezvestných detí, v prípade ktorých bolo nahlásené podozrenie z únosu dieťaťa a začalo sa trestné stíhanie pod dohľadom súdneho orgánu a v prípade ktorých bolo vydané upozornenie na únos dieťaťa. Podmienky stanovené zákonom pre naplnenie databázy majú za cieľ prísne obmedziť počet dotknutých osôb a osobných údajov, ktoré sa majú zahrnúť do databázy. Nositeľ rodičovských práv a povinností vo vzťahu k dieťaťu musí byť informovaný o vykonanom spracúvaní a o podmienkach výkonu práv dieťaťa v súvislosti s biometrickým spracúvaním plánovaným na účely identifikácie alebo o osobných údajoch dieťaťa uchovávaných v databáze.

### 2.4. Záver

Vzhľadom na nevyhnutnosť a primeranosť plánovaného spracúvania, ako aj na najlepší záujem dieťaťa pri vykonávaní takéhoto spracúvania osobných údajov a za predpokladu, že sú zavedené dostatočné záruky najmä na zabezpečenie výkonu práv dotknutej osoby – najmä s prihliadnutím na skutočnosť, že sa majú spracúvať údaje detí – možno takéto vykonávanie spracúvania na základe rozpoznávania tváre považovať za pravdepodobne zlučiteľné s právom EÚ.

Okrem toho vzhľadom na typ spracúvania a použitú technológiu, ktorá predstavuje vysoké riziko pre práva a slobody tejto dotknutej osoby, sa EDPB domnieva, že príprava návrhu legislatívneho opatrenia, ktoré má prijať národný parlament, alebo regulačného opatrenia založeného na takomto legislatívnom opatrení, ktoré sa týka plánovaného spracúvania, musí zahŕňať predchádzajúcu konzultáciu dozorného orgánu s cieľom zabezpečiť konzistentnosť a súlad s uplatniteľným právnym rámcom, pozri článok 28 ods. 2 LED.

## 3 SCENÁR 3

### 3.1. Popis

V priebehu policajných zásahov z dôvodu nepokojov a následných vyšetrovaní bolo niekoľko osôb identifikovaných ako podozrivé osoby, napr. na základe predchádzajúcich vyšetrovaní s využitím pokrytia kamerových systémov alebo svedkov. Fotografie týchto podozrivých osôb sa porovnávajú s fotografiami osôb, ktoré boli zaznamenané na kamerových záznamoch alebo mobilných zariadeniach na mieste činu alebo v okolí.

S cieľom získať podrobnejšie dôkazy o osobách podozrivých z účasti na nepokojoch, ktoré sprevádzali demonštráciu, polícia vytvára databázu pozostávajúcu z obrazového materiálu s približnou súvislosťou s miestom a časom nepokojov. Databáza obsahuje súkromné záznamy, ktoré občania poskytli polícii, materiál z kamerového systému verejnej dopravy, materiál zo sledovania kamerovým systémom vo vlastníctve polície a materiál uverejňovaný médiami bez akéhokoľvek konkrétneho obmedzenia alebo záruky. Zobrazovanie závažnej trestnej činnosti nie je nevyhnutným predpokladom zhromažďovania súborov v databáze. Preto sú v databáze uložené aj osoby, ktoré sa nezúčastnili na nepokojoch – významné percento miestneho obyvateľstva, ktoré sa v čase demonštrácie náhodou ocitlo v blízkosti, alebo sa zúčastnilo demonštrácie, ale nie na nepokojoch. Ide o tisíce videozáznamov a obrazových súborov.

Pomocou softvéru na rozpoznávanie tvárí sa všetkým tvárám, ktoré sa v týchto súboroch objavia, priradí jedinečný identifikátor tváre. Tváre jednotlivých podozrivých osôb sa potom automaticky porovnávajú s týmito identifikátormi tváre. Databáza pozostávajúca zo všetkých biometrických vzorov v tisícoch videozáznamov a obrazových súborov sa uchováva až do ukončenia všetkých možných

vyšetrovaní. Pozitívnymi zhodami sa zaoberajú zodpovední príslušníci, ktorí potom rozhodnú o ďalších opatreniach. To môže zahŕňať priradenie súboru nachádzajúceho sa v databáze k trestnému spisu príslušnej osoby, ako aj ďalšie opatrenia, ako je vypočúvanie alebo zatknutie tejto osoby.

Vo vnútroštátnom práve sa uvádza všeobecné ustanovenie, podľa ktorého je spracúvanie biometrických údajov na účely individuálnej identifikácie fyzickej osoby prípustné, ak je to úplne nevyhnutné a podlieha primeraným zárukám ochrany práv a slobôd dotknutej osoby.

Zdroj informácií:

- Typy dotknutých osôb: ☒ všetky osoby
- Zdroj snímky: ☒ verejne prístupné priestory ☒ súkromný subjekt ☒ iné osoby ☒ iné: médiá
- Súvislosť s trestnou činnosťou :☒ nie nevyhnutne priama geografická alebo časová súvislosť
- Spôsob zachytávania informácií:☒ na diaľku
- Kontext - vplyv na iné základné práva: Áno, konkrétne ☒ v kontexte slobody zhromažďovania.
- Dostupné ďalšie zdroje informácií o dotknutej osobe:
  ☒ iné: nie je vylúčené (napríklad používanie bankomatov alebo vstup do obchodov), pretože nie je možné kontrolovať motívy zachytené na obrazoch

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť: ☒ špecifické databázy týkajúce sa oblasti trestnej činnosti

Algoritmus:

- Typ spracúvania: ☒ identifikácia jedna k mnohým

Výsledok:

- Vplyv: ☒ priamy (napr. dotknutá osoba môže byť zatknutá, vypočúvaná);
- Automatizované rozhodovanie: ☒ NIE
- Doba uchovávania: do ukončenia všetkých možných vyšetrovaní

Právna analýza:

- Typ predbežných informácií pre dotknutú osobu: ☒ Všeobecne na webovom sídle OPP
- Uplatniteľný právny rámec : ☒ LED väčšinou skopírovaná do vnútroštátneho práva ☒ všeobecné vnútroštátne právne predpisy o používaní biometrických údajov OPP

## 3.2. Uplatniteľný právny rámec

Ako bolo objasnené vyššie, právne základy, ktoré len opakujú všeobecné ustanovenie článku 10 LED nie sú dostatočne jasné na to, aby jednotlivcom poskytli primerané informácie o podmienkach a okolnostiach, za ktorých sú OPP oprávnené používať záznamy z kamerových systémov na verejných priestranstvách na vytvorenie biometrického vzoru ich tváre a porovnať ju s policajnými databázami, inými dostupnými kamerovými systémami alebo súkromnými záznamami atď. Právny rámec stanovený v tomto scenári preto nespĺňa minimálne požiadavky, aby mohol slúžiť ako právny základ.

## 3.3. Nevyhnutnosť a primeranosť

V tomto príklade spracúvanie vyvoláva rôzne obavy vzhľadom na zásady nevyhnutnosti a primeranosti z viacerých dôvodov:

Osoby nie sú podozrivé zo závažného trestného činu. Zobrazenie závažnej trestnej činnosti nie je predpokladom používania súborov v databáze, ktoré obsahujú obrazový materiál. Priama časová a

geografická súvislosť s trestným činom tiež nie je predpokladom na použitie súborov v databáze. Výsledkom je, že značný percentuálny podiel miestneho obyvateľstva sa uchováva v biometrickej databáze potenciálne po dobu niekoľko rokov, a to až do ukončenia všetkých vyšetrovaní.

Databáza miest činu nie je obmedzená na obrazy spĺňajúce požiadavky na primeranosť, čo vedie k neobmedzenému množstvu obrazov na porovnanie. Je to v rozpore so zásadou minimalizácie údajov. Menšie množstvo obrazov by skôr umožnilo zvážiť nealgoritmické a menej rušivé prostriedky, napr. osoby so superschopnosťou rozpoznávania.[88]

Keďže tento príklad pochádza z okolia protestu, je pravdepodobné, že obrazy odhaľujú aj politické názory účastníkov demonštrácie, čo je druhá osobitná kategória údajov, ktorá môže byť týmto scenárom ovplyvnená. V tomto scenári nie je jasné, ako sa dá zabrániť zhromažďovaniu takýchto údajov a s akými zárukami. Okrem toho, ak sa dotknuté osoby dozvedia, že ich účasť na demonštrácii viedla k ich zaznamenaniu do biometrickej databázy polície, môže to mať vážne odstrašujúce účinky pri ich budúcom uplatňovaní práva na zhromažďovanie.

Biometrické vzory v databáze možno takisto navzájom porovnávať. To umožňuje polícii nielen hľadať konkrétnu osobu vo všetkých materiáloch, ale aj rekonštruovať vzorec správania osoby počas niekoľkých dní. Môže tiež získavať ďalšie informácie o osobách, ako sú sociálne kontakty a politické zapojenie.

Zásah je okrem toho o to hlbší, že údaje sa spracúvajú bez vedomia dotknutých osôb.

Ak si uvedomíme, že ľudia neustále zaznamenávajú fotografie a videozáznamy a že aj všadeprítomné kamerové záznamy môžu byť biometricky analyzované, môže to viesť k závažným odstrašujúcim účinkom.

Ďalším zdrojom obáv je rozsiahle využívanie súkromných fotografií a videozáznamov vrátane možného zneužitia, ako je napríklad udanie. Keďže zneužitie, ako je udanie, je rizikom, ktoré sa aj vo všeobecnosti spája s trestným konaním, riziko je podstatne vyššie, pokiaľ ide o rozsah spracúvaných údajov a počet zapojených osôb, keďže ľudia môžu nahrať aj materiál týkajúci sa konkrétnej osoby alebo skupiny osôb, ktoré sa im nepáčia. Žiadosti polície o poskytnutie fotografií a videozáznamov môžu viesť k veľmi nízkym zábranám pre ľudí, ktorí chcú materiál poskytnúť, najmä preto, že by to mohlo byť možné urobiť anonymne alebo aspoň bez potreby dostaviť sa na policajnú stanicu a preukázať svoju totožnosť.

### 3.4. Záver

V tomto príklade neexistuje žiadne konkrétne ustanovenie, ktoré by mohlo slúžiť ako právny základ. Aj keby však existoval dostatočný právny základ, požiadavky nevyhnutnosti a primeranosti by neboli splnené, čo by viedlo k neprimeranému zásahu do práv dotknutej osoby na rešpektovanie súkromného života a ochranu osobných údajov podľa Charty.

## 4 SCENÁR 4

### 4.1. Popis

Polícia zavádza spôsob identifikácie podozrivých zo spáchania závažného trestného činu zaznamenaného kamerovým systémom spätným použitím TRT. Pracovník manuálne vyberie snímok (snímky) podozrivých z videozáznamu, ktorý bol získaný z miesta činu alebo inde v rámci predbežného

[88] T. j. ľudia s mimoriadnou schopnosťou rozpoznávať tváre. Pozri tiež: Face Recognition by Metropolitan Police Super-Recognisers, 26. februára 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

vyšetrovania, a potom odošle snímok (snímky) forenznému oddeleniu. Forenzné oddelenie používa TRT na porovnanie týchto snímok s fotografiami osôb, ktoré polícia predtým zhromaždila v databáze (tzv. databáza opisov, ktorá pozostáva z podozrivých a bývalých odsúdených). Databáza opisov je pri tomto postupe – dočasne a v izolovanom prostredí – analyzovaná pomocou FRT, aby bolo možné vykonať porovnanie. S cieľom minimalizovať zásah do práv a záujmov porovnávaných osôb má veľmi obmedzený počet zamestnancov forenzného oddelenia povolenie na vykonanie samotného postupu porovnávania, prístup k údajom je obmedzený na úradníkov poverených konkrétnym spisom a pred postúpením akéhokoľvek výsledku vyšetrujúcemu úradníkovi sa vykonáva manuálna kontrola výsledkov. Biometrické údaje sa neposielajú mimo kontrolovaného, izolovaného prostredia. Pri vyšetrovaní sa ďalej používa len výsledok a fotografia (nie biometrický vzor). Zamestnanci absolvujú osobitnú odbornú prípravu týkajúcu sa pravidiel a postupov tohto spracúvania a každé spracúvanie osobných a biometrických údajov je dostatočne špecifikované vo vnútroštátnych právnych predpisoch.

Zdroj informácií:

- Typy dotknutých osôb: ☒ podozrivé osoby identifikované na základe záznamov z kamerových systémov
- Zdroj snímky: ☒ verejne prístupné priestory ☒ internet
- Súvislosť s trestnou činnosťou: ☒ Priama časová
  ☒ Priama geografická
- Spôsob zachytávania informácií:☒ na diaľku
- Kontext – vplyv na iné základné práva: Áno, konkrétne: ☒ sloboda zhromažďovania ☒ sloboda prejavu ☒ rôzne: __

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť: ☒ špecifické databázy týkajúce sa oblasti trestnej činnosti

Algoritmus:

- Typ spracúvania: ☒ identifikácia jedna k mnohým

Výsledok:

- Vplyv: ☒ priamy (napr. dotknutá osoba je zatknutá, vypočúvaná)
- Automatizované rozhodnutie: ☒ NIE

Právna analýza:

- Uplatniteľný právny rámec : ☒ Osobitné vnútroštátne právne predpisy pre toto spracúvanie (rozpoznávanie tváre) pre daný príslušný orgán

## 4.2. Uplatniteľný právny rámec

V tomto scenári je vo vnútroštátnom práve stanovené, že biometrické údaje sa môžu použiť pri vykonávaní forenznej analýzy, ak je to úplne nevyhnutné na dosiahnutie účelu identifikácie podozrivých osôb, ktoré spáchali závažný trestný čin, prostredníctvom porovnania fotografií v databáze opisov. Vo vnútroštátnych právnych predpisoch sa stanovuje, ktoré údaje sa môžu spracúvať, ako aj postupy na zachovanie integrity a dôvernosti osobných údajov a postupy na ich zničenie, čím sa poskytujú dostatočné záruky proti riziku zneužitia a svojvoľnosti.

## 4.3. Nevyhnutnosť a primeranosť

Používanie rozpoznávania tváre je jednoznačne časovo efektívnejšie ako manuálne porovnávanie na forenznej úrovni. Predchádzajúci manuálny výber snímok obmedzuje zásah v porovnaní

s porovnávaním celého videozáznamu s databázou, a tým rozlišuje a zameriava sa len na osoby, na ktoré sa vzťahuje príslušný cieľ, t. j. boj proti závažnej trestnej činnosti. V závislosti od konkrétneho prípadu je však stále dôležité zvážiť, či by porovnanie nebolo možné v primeranom čase vykonať manuálne. Obmedzenie počtu osôb s prístupom k technológii a osobným údajom znižuje vplyv na práva na súkromie a ochranu údajov, okrem toho sa biometrické vzory takto neuchovávajú ani nepoužívajú neskôr počas vyšetrovania. Manuálna kontrola výsledku znamená aj znížené riziko akýchkoľvek falošne pozitívnych výsledkov.

### 4.4. Záver

Je dôležité, aby vnútroštátne právne predpisy poskytovali primeraný právny základ pre spracúvanie biometrických údajov, ako aj pre vnútroštátnu databázu, s ktorou sa uskutočňuje porovnávanie. V tomto scenári bolo zavedených niekoľko opatrení s cieľom obmedziť zasahovanie do práv na ochranu údajov, ako sú podmienky používania TRT stanovené v právnom základe, počet osôb s prístupom k tejto technológii a biometrickým údajom, manuálne kontroly atď. TRT výrazne zlepšuje efektívnosť vyšetrovacej práce forenzného oddelenia polície, je založená na právnych predpisoch umožňujúcich polícii spracúvať biometrické údaje, ak je to absolútne nevyhnutné, a preto sa v rámci týchto parametrov môže považovať za zákonný zásah do práv jednotlivca.

## 5 SCENÁR 5

### 5.1. Popis

Diaľková biometrická identifikácia je situácia, keď sa totožnosť osôb stanovuje pomocou biometrických identifikátorov (snímky tváre, chôdza, dúhovka atď.) na diaľku, vo verejnom priestore, nepretržitým alebo priebežným spôsobom, a to ich porovnaním s (biometrickými) údajmi uchovávanými v databáze[89]. Diaľková biometrická identifikácia sa vykonáva v reálnom čase, ak zachytenie obrazového materiálu, porovnanie a identifikácia prebiehajú bez výrazného oneskorenia.

Pred každým použitím diaľkovej biometrickej identifikácie v reálnom čase polícia zostaví v rámci vyšetrovania zoznam záujmových osôb [watch list]. Napĺňa sa snímkami tváre jednotlivcov. Na základe spravodajských informácií, z ktorých vyplýva, že sa osoby budú nachádzať v určitej oblasti, napríklad v nákupnom centre alebo na verejnom priestranstve, polícia rozhodne, kedy, kde a ako dlho bude používať diaľkovú biometrickú identifikáciu.

V deň akcie sa na mieste umiestni policajná dodávka ako riadiace centrum, v ktorej sa bude nachádzať vyšší policajný dôstojník. V dodávke sú monitory, na ktorých sa zobrazujú záznamy z kamerových systémov umiestnených v blízkosti, ktoré sa buď inštalujú na mieste alebo pripojením k prenosom videa už nainštalovaných kamier. Keď chodci prechádzajú okolo kamier, technológia izoluje snímky tváre, konvertuje ich na biometrické vzory a porovnáva ich s biometrickými vzormi osôb na zozname sledovaných osôb.

Ak sa zistí potenciálna zhoda medzi zoznamom sledovaných osôb a osobami prechádzajúcimi okolo kamier, vyšle sa upozornenie policajtom v dodávke, ktorí potom informujú policajtov na mieste, ak je upozornenie pozitívne, napr. prostredníctvom rádiového zariadenia. Policajt na mieste sa potom rozhodne, či zasiahne, priblíži sa k osobe alebo ju v konečnom dôsledku zadrží. Opatrenia prijaté policajtom na mieste sa zaznamenávajú. V prípade diskrétnej kontroly sa získané informácie (napr. s kým je osoba, čo majú oblečené a kam smerujú) uchovávajú.

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

Vo vnútroštátnom práve, na ktoré sa odkazuje, sa uvádza všeobecné ustanovenie, podľa ktorého je spracúvanie biometrických údajov na účely individuálnej identifikácie fyzickej osoby prípustné, ak je to úplne nevyhnutné a podlieha primeraným zárukám ochrany práv a slobôd dotknutej osoby.

Zdroj informácií:

- Typy dotknutých osôb: ☒ všetky osoby
- Zdroj snímky: ☒ verejne prístupné priestory
- Súvislosť s trestnou činnosťou: ☒ nie nevyhnutne priama geografická alebo časová súvislosť
- Spôsob zachytávania informácií: ☒ na diaľku
- Kontext – vplyv na iné základné práva: Áno, konkrétne: ☒ sloboda zhromažďovania ☒ sloboda prejavu ☒ rôzne
- Dostupné ďalšie zdroje informácií o dotknutej osobe:
  ☒ iné: nevylúčené (napríklad používanie bankomatov alebo vstup do obchodov)

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť: ☒ špecifické databázy týkajúce sa oblasti trestnej činnosti

Algoritmus:

- Typ spracúvania: ☒ identifikácia jedna k mnohým

Výsledok:

- Vplyv: ☒ priamy (napr. dotknutá osoba je zatknutá, vypočúvaná)
- Automatizované rozhodnutie: ☒ NIE
- Doba uchovávania: do ukončenia všetkých možných vyšetrovaní

Právna analýza:

- Typ predbežných informácií pre dotknutú osobu: ☒ Všeobecne na webovom sídle OPP
- Uplatniteľný právny rámec: ☒ LED väčšinou skopírovaná do vnútroštátneho práva ☒ všeobecné vnútroštátne právne predpisy o používaní biometrických údajov OPP

## 5.2. Uplatniteľný právny rámec

Právne základy, ktoré len opakujú všeobecné ustanovenie článku 10 LED, nie sú dostatočne jasné na to, aby jednotlivcom poskytli primerané informácie o podmienkach a okolnostiach, za ktorých sú OPP oprávnené používať záznamy z kamerových systémov na verejných priestranstvách na vytvorenie biometrického vzoru ich tváre a porovnať ju s policajnými databázami. Právny rámec stanovený v tomto scenári preto nespĺňa minimálne požiadavky na to, aby slúžil ako právny základ.[90]

## 5.3. Nevyhnutnosť a primeranosť

Latka pre nevyhnutnosť a primeranosť je nastavená tým vyššie, čím je zásah hlbší. Diaľková biometrická identifikácia na verejných priestranstvách má niekoľko dôsledkov pre základné práva:

Scenáre zahŕňajú monitorovanie každého okoloidúceho v príslušnom verejnom priestore. Závažne sa tým ovplyvňuje oprávnené očakávanie obyvateľstva na anonymitu na verejných priestranstvách[91]. To

[90] V prípadoch, že by vedecký projekt zameraný na výskum používania TRT potreboval spracúvať osobné údaje, ale takéto spracúvanie by nespadalo pod článok 4 ods. 3 LED alebo by bolo mimo rozsahu pôsobnosti práva Únie, bolo by uplatniteľné všeobecné nariadenie o ochrane údajov. V prípade pilotných projektov, po ktorých by nasledovali operácie presadzovania práva, by sa LED taktiež uplatňovala.

[91] Odpoveď EDPB poslancom Európskeho parlamentu týkajúca sa aplikácie na rozpoznávanie tváre vyvinutej spoločnosťou Clearview AI, 10. júna 2020, Ref: OUT2020-0052.

je predpokladom pre mnohé aspekty demokratického procesu, ako napríklad rozhodnutie vstúpiť do občianskeho združenia, navštíviť zhromaždenia a stretnúť sa s ľuďmi z rôznych sociálnych a kultúrnych prostredí, zúčastniť sa na politickom proteste a navštíviť miesta rôzneho druhu. Pojem anonymity vo verejnom priestore je nevyhnutný pre slobodné zhromažďovanie a výmenu informácií a myšlienok. Zachováva pluralitu názorov, slobodu pokojného zhromažďovania a slobodu združovania a ochranu menšín a podporuje zásady oddelenia právomocí a systémy bŕzd a protiváh. Podkopávanie koncepcie anonymity na verejných priestranstvách môže mať za následok vážny odstrašujúci účinok na občanov. Môžu sa zdržiavať určitého správania, ktoré je v medziach slobodnej a otvorenej spoločnosti. To by ovplyvnilo verejný záujem, keďže demokratická spoločnosť si vyžaduje sebaurčenie a účasť občanov na demokratickom procese.

Ak sa takáto technológia používa, už len obyčajná prechádzka po ulici, do metra alebo do pekárne v dotknutej oblasti povedie k zhromažďovaniu osobných údajov vrátane biometrických údajov orgánmi presadzovania práva a v prvom scenári aj k porovnaniu s policajnými databázami. Situácia, v ktorej by sa to isté vykonalo odobratím odtlačkov prstov, by bola zjavne neprimeraná.

Počet dotknutých osôb, ktorých sa to týka, je mimoriadne vysoký, pretože každý, kto prechádza cez príslušnú verejnú oblasť, je ovplyvnený. Okrem toho by tieto scenáre znamenali automatizované hromadné spracúvanie biometrických údajov a tiež hromadné porovnávanie biometrických údajov s policajnými databázami.

V európskej judikatúre je hromadné sledovanie zakázané (napr. ESĽP vo veci S. a Marper proti Spojenému kráľovstvu považoval nediferencované uchovávanie biometrických údajov za „neprimeraný zásah“ do práva na súkromie, keďže ho nemožno považovať za „nevyhnutné v demokratickej spoločnosti“).

Diaľková biometrická identifikácia má takú tendenciu k hromadnému sledovaniu, že neexistujú žiadne spoľahlivé prostriedky na jej obmedzenie. Zásadne sa líši od sledovania pomocou kamerového systému ako takého, pretože už možné použitie videozáznamu bez biometrickej identifikácie je závažným zásahom, ale zároveň zásahom obmedzeným, zatiaľ čo v prípade uplatnenia TRT dôjde k zmene charakteru už rozšíreného sledovania pomocou kamerového systému ako hlavného zdroja údajov. Okrem toho, najmä s ohľadom na možné odstrašujúce účinky, prípadné obmedzenia používania už existujúcich zariadení sledovania kamerovým systémom nebudú viditeľné, a teda verejnosť im nebude dôverovať.

V prípade diaľkovej biometrickej identifikácie policajnými orgánmi sa ku každému pristupuje ako k potenciálnemu podozrivému. V právnom štáte sa však občania považujú za nevinných, kým sa nepreukáže ich pochybenie. Táto zásada sa čiastočne odráža aj v LED, ktorá zdôrazňuje potrebu rozlišovať, pokiaľ je to možné, medzi zaobchádzaním s odsúdenými alebo podozrivými z trestnej činnosti, v prípade ktorých sa musia orgány činné v trestnom konaní „*odôvodnene domnievať, že spáchali alebo sa chystajú spáchať trestný čin;*“ [článok 6 písm. a) LED], v porovnaní s tými, ktorí nie sú odsúdení alebo podozriví z trestnej činnosti.

V prípade uplatnenia v kľúčových dopravných uzloch alebo verejných priestoroch, pričom OPP používajú technológiu, ktorá dokáže jedinečne identifikovať jednu osobu a vysledovať a analyzovať miesto jej pobytu a pohybov, sa odhalia tie najcitlivejšie informácie o osobe (dokonca aj o sexuálnych preferenciách, náboženstve, zdravotných problémoch). Vzniká tak obrovské riziko nezákonného prístupu k údajom a ich neoprávneného využívania.

Zavedenie systému, ktorý umožňuje odhaliť samotnú podstatu správania a vlastností jednotlivca, vedie k silným odstrašujúcim účinkom. Núti ľudí pochybovať o tom, či sa majú pridať k určitej manifestácii,

čím poškodzuje demokratický proces. Za kritické môže byť považované aj stretnutie s určitým priateľom, o ktorom je známe, že má problémy s políciou alebo sa správa neštandardným spôsobom, keďže toto všetko by viedlo k upútaniu pozornosti algoritmu systému, a teda presadzovania práva.

Neexistuje tu možnosť chrániť zraniteľné dotknuté osoby, ako sú deti. Okrem toho sú dotknuté aj osoby ako sú novinári, právnici a duchovní, ktorí majú profesionálny záujem – a často aj zodpovedajúcu právnu povinnosť – zachovať dôvernosť svojich kontaktov. Mohlo by to viesť napríklad k odhaleniu zdroja a novinára alebo odhaleniu toho, že osoba sa radí s trestnoprávnym obhajcom. Tento problém sa netýka len náhodných verejných miest, kde sa stretávajú napr. novinári a ich zdroje, ale prirodzene aj verejných priestorov potrebných na oslovenie inštitúcií alebo odborníkov a prístup k nim.

Nepríjemné pocity ľudí v súvislosti s TRT môžu okrem toho viesť k zmene ich správania, vyhýbaniu sa miestam, kde sa TRT používa, a tým aj k ich stiahnutiu sa zo spoločenského života a kultúrnych podujatí. V závislosti od rozsahu používania TRT môže byť vplyv na ľudí taký výrazný, že ovplyvní ich schopnosť viesť dôstojný život[92].

Preto existuje veľká pravdepodobnosť, že ovplyvní podstatu – nedotknuteľné jadro – práva na ochranu osobných údajov. Ide najmä o tieto silné náznaky (pozri oddiel 3.1.3.2 usmernení): OPP vo veľkom rozsahu automaticky spracúvajú jedinečné biologické vlastnosti ľudí pomocou algoritmov založených na hodnovernosti s len obmedzenou vysvetliteľnosťou výsledkov. Obmedzenia práva na súkromie a ochranu údajov sa uplatňujú bez ohľadu na individuálne správanie osoby alebo okolnosti, ktoré sa jej týkajú. Štatisticky takmer všetky dotknuté osoby ovplyvnené týmto zásahom sú jednotlivci dodržiavajúci právne predpisy. Existujú len obmedzené možnosti poskytovania informácií dotknutej osobe. Súdne opravné prostriedky vo väčšine prípadov budú k dispozícii až následne.

Spoliehanie sa na systém založený na hodnovernosti a s obmedzenou vysvetliteľnosťou môže viesť k zahmleniu zodpovednosti a nedostatku v oblasti nápravy a môže byť impulzom k nedbanlivosti.

Keď sa takýto systém, ktorý sa dá použiť aj pri existujúcich kamerových systémoch, použije, môže sa s minimálnym úsilím a bez toho, aby bol viditeľný pre jednotlivcov, zneužiť a umožniť systematické a rýchle zostavovanie zoznamov osôb podľa etnického pôvodu, pohlavia, náboženstva atď. Zásada spracúvania osobných údajov na základe vopred stanovených kritérií, ako je miesto pobytu osoby a prejdená trasa, sa už uplatňuje[93] a je náchylná k diskriminácii.

Vzhľadom na citlivosť, výpovednú hodnotu a množstvo spracúvaných údajov sú systémy na diaľkové rozpoznávanie tváre na verejne prístupných miestach náchylné na zneužitie so škodlivými účinkami pre dotknutých jednotlivcov. Takéto údaje sa takisto môžu ľahko získavať a zneužívať na vyvíjanie tlaku na kľúčových aktérov v rámci systému bŕzd a protiváh, ako sú politická opozícia, úradníci a novinári.

Napokon, systémy TRT majú tendenciu zahŕňať silné účinky zaujatosti týkajúce sa rasy a pohlavia: falošne pozitívne výsledky neúmerne ovplyvňujú osoby inej farby pleti a ženy[94], čo vedie k diskriminácii.

---

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

[93] Pozri článok 6 smernice Európskeho parlamentu a Rady (EÚ) 2016/681 z 27. apríla 2016 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti a článok 33 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1240 z 12. septembra 2018, ktorým sa zriaďuje Európsky systém pre cestovné informácie a povolenia (ETIAS) a ktorým sa menia nariadenia (EÚ) č. 1077/2011, (EÚ) č. 515/2014, (EÚ) 2016/399, (EÚ) 2016/1624 a (EÚ) 2017/2226.

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

Policajné opatrenia na základe falošne pozitívnych výsledkov, ako sú prehliadky a zatknutia, ďalej stigmatizujú tieto skupiny.

### 5.4. Záver

Uvedené scenáre týkajúce sa diaľkového spracúvania biometrických údajov vo verejných priestoroch na účely identifikácie nevytvárajú spravodlivú rovnováhu medzi navzájom si konkurujúcimi súkromnými a verejnými záujmami, a teda predstavujú neprimerané zasahovanie do práv dotknutej osoby podľa článkov 7 a 8 Charty.

## 6 SCENÁR 6

### 6.1. Popis

Súkromný subjekt poskytuje aplikáciu, v ktorej sa z internetu extrahujú snímky tvárí na vytvorenie databázy. Používateľ, napr. polícia, potom môže nahrať fotografiu a aplikácia sa ju pomocou biometrickej identifikácie pokúsi porovnať so snímkami tváre alebo biometrickými vzormi vo svojej databáze.

Miestne policajné oddelenie vedie vyšetrovanie trestného činu zachyteného na videozázname, pri ktorom nie je možné identifikovať viacero potenciálnych svedkov a podozrivých porovnaním získaných informácií so žiadnou internou databázou alebo spravodajskými informáciami. Jednotlivci nie sú na základe zhromaždených informácií registrovaní v žiadnej existujúcej policajnej databáze. Polícia sa rozhodne použiť nástroj uvedený vyššie, ktorý poskytuje súkromná spoločnosť, na identifikáciu jednotlivcov prostredníctvom biometrickej identifikácie.

Zdroj informácií:

- Typy dotknutých osôb: ☒ všetci občania (svedkovia) ☒ odsúdené osoby ☒ podozrivé osoby
- Zdroj snímky: ☒ videozáznam z verejného priestranstva alebo získaný inde v rámci predbežného vyšetrovania
- Spojenie s trestnou činnosťou: ☒ nemusí byť
- Spôsob zachytávania informácií: ☒ na diaľku
- Kontext – vplyv na iné základné práva: Áno, konkrétne: ☒ sloboda zhromažďovania ☒ sloboda prejavu ☒ rôzne __

Referenčná databáza (s ktorou sa porovnávajú zachytené informácie):

- Špecifickosť: ☒ databázy na všeobecné účely naplnené z internetu

Algoritmus:

- Typ spracúvania: ☒ identifikácia jedna k mnohým

Výsledok:

- Vplyv ☒ priamy (napr. zatknutie dotknutej osoby, vypočúvanie, diskriminačné správanie)
- Automatizované rozhodnutie: ☒ NIE

Právna analýza:

- Typ predbežných informácií pre dotknutú osobu: ☒ Nie

## 6.2. Uplatniteľný právny rámec

Ak súkromný subjekt poskytuje službu, ktorá zahŕňa spracúvanie osobných údajov, pre ktoré určuje účel a prostriedky (v tomto prípade extrahovanie snímok z internetu na vytvorenie databázy), tento súkromný subjekt musí mať pre toto spracúvanie právny základ. Okrem toho OPP, ktorý sa rozhodne používať túto službu na svoje účely, musí mať právny základ pre spracúvanie, pre ktorý určí účely a prostriedky. Na to, aby OPP mohol spracúvať biometrické údaje, musí existovať právny rámec, ktorý špecifikuje cieľ, osobné údaje, ktoré sa majú spracúvať, účely spracúvania a postupy na zachovanie integrity a dôvernosti osobných údajov, ako aj postupy na ich likvidáciu.

Tento scenár predpokladá hromadné získavanie osobných údajov od jednotlivcov, ktorí si nie sú vedomí toho, že ich údaje sa získavajú. Takéto spracúvanie by mohlo byť zákonné len za veľmi výnimočných okolností. V závislosti od toho, kde sa databáza nachádza, môže používanie takejto služby znamenať prenos osobných údajov a/alebo osobitných kategórií osobných údajov mimo Európskej únie (napríklad ak polícia „odošle“ snímku tváre na videozázname zo sledovania alebo inak získané), čo si vyžaduje osobitné podmienky pre tento prenos, pozri článok 39 LED.

V tomto scenári neexistujú žiadne osobitné pravidlá, ktoré by umožnili toto spracúvanie zo strany OPP.

## 6.3. Nevyhnutnosť a primeranosť

Využívanie služby zo strany OPP znamená, že osobné údaje sa zdieľajú so súkromným subjektom, ktorý využíva databázu, v ktorej sa osobné údaje zhromažďujú, neobmedzeným, hromadným spôsobom. Neexistuje žiadna súvislosť medzi získanými osobnými údajmi a sledovaným cieľom OPP. Zdieľanie údajov zo strany OPP súkromnému subjektu znamená aj nedostatočnú kontrolu tohto orgánu nad údajmi spracúvanými súkromným subjektom a veľké ťažkosti pre dotknuté osoby pri uplatňovaní ich práv, keďže nebudú vedieť o tom, že ich údaje sa týmto spôsobom spracúvajú. Nastavuje sa tým veľmi vysoká latka pre situácie, v ktorých by k takémuto spracúvaniu vôbec mohlo dôjsť. Je otázne, či by akýkoľvek cieľ spĺňal požiadavky stanovené v smernici (pozn.: LED), keďže akékoľvek výnimky a obmedzenia práv na súkromie a ochranu údajov sa uplatňujú len vtedy, keď je to úplne nevyhnutné. Všeobecný záujem o účinnosť boja proti závažným trestným činom nemôže sám osebe odôvodniť spracúvanie, ak sa takéto obrovské množstvo údajov zbiera nediferencovaným spôsobom. Toto spracúvanie by preto nespĺňalo požiadavky nevyhnutnosti a primeranosti.

## 6.4. Záver

Chýbajúce jasné, presné a predvídateľné pravidlá, ktoré spĺňajú požiadavky uvedené v článkoch 4 a 10 smernice (pozn.: LED), a chýbajúce dôkazy o tom, že toto spracúvanie je úplne nevyhnutné na dosiahnutie zamýšľaných cieľov, vedú k záveru, že použitie tejto aplikácie by nespĺňalo požiadavky nevyhnutnosti a primeranosti a znamenalo by neprimeraný zásah do práv dotknutých osôb na rešpektovanie súkromného života a ochranu osobných údajov podľa Charty.