Smjernice

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Smjernice 5/2022 o upotrebi tehnologije prepoznavanja lica u području izvršavanja zakonodavstva

Inačica 2.0.

Doneseno 26. travnja 2023.

Povijest inačice

Inačica 1.0.	12. svibnja 2022.	Donošenje Smjernica za potrebe savjetovanja s javnošću
Inačica 2.0.	26. travnja 2023.	Donošenje Smjernica nakon savjetovanja s javnošću

Sadržaj

SAŽETAK

Sve više tijela za izvršavanje zakonodavstva primjenjuje ili namjerava primjenjivati tehnologiju prepoznavanja lica. Ta se tehnologija može upotrebljavati za **autentifikaciju** ili **identifikaciju** osobe te se može primjenjivati na videozapise (npr. CCTV) ili fotografije. Može se upotrebljavati u različite svrhe, među ostalim za traganje za osobama na policijskim popisima za praćenje ili za praćenje kretanja osobe u javnom prostoru.

Tehnologija prepoznavanja lica temelji se na obradi **biometrijskih podataka**, što znači da obuhvaća obradu posebnih kategorija osobnih podataka. Tehnologija prepoznavanja lica često upotrebljava sastavnice **umjetne inteligencije** ili strojnog učenja. Iako se time omogućuje opsežna obrada podataka, također se stvara rizik od diskriminacije i lažnih rezultata. Tehnologija prepoznavanje lica može se upotrebljavati u kontroliranim situacijama 1:1, ali i u golemim skupinama ljudi i na važnim prometnim čvorištima.

Tehnologija prepoznavanja lica **osjetljiv je alat za tijela za izvršavanje zakonodavstva.** Tijela za izvršavanje zakonodavstva izvršna su tijela i imaju suverene ovlasti. Tehnologija prepoznavanja lica mogla bi zadirati u temeljna prava čak i izvan opsega prava na zaštitu osobnih podataka, te može utjecati na našu društvenu i demokratsku političku stabilnost.

Za zaštitu osobnih podataka u kontekstu izvršavanja zakonodavstva moraju se ispuniti **zahtjevi Direktive o zaštiti podataka pri izvršavanju zakonodavstva**. Direktivom o zaštiti podataka pri izvršavanju zakonodavstva predviđen je određeni okvir u pogledu upotrebe tehnologije prepoznavanja lica, osobito u njezinu članku 3. stavku 13. („biometrijski podaci"), članku 4. (načela obrade osobnih podataka), članku 8. (zakonitost obrade), članku 10. (obrada posebnih kategorija osobnih podataka) i članku 11. (automatizirano pojedinačno donošenje odluka).

Primjena tehnologije prepoznavanja lica također može utjecati na nekoliko drugih temeljnih prava. Stoga je **Povelja EU-a o temeljnim pravima** (u daljnjem tekstu: Povelja) ključna za tumačenje Direktive o zaštiti podataka pri izvršavanju zakonodavstva, osobito u pogledu prava na zaštitu osobnih podataka iz članka 8. Povelje, ali i prava na privatnost utvrđenog u članku 7. Povelje.

Zakonodavne mjere koje služe kao pravna osnova za obradu osobnih podataka izravno utječu na prava zajamčena člancima 7. i 8. Povelje. Obrada biometrijskih podataka u svim okolnostima sama po sebi predstavlja teško zadiranje u prava. To ne ovisi o ishodu, npr. pronalasku podudaranja. Svako ograničenje ostvarivanja temeljnih prava i sloboda mora biti predviđeno zakonom i njime se mora poštovati suština tih prava i sloboda.

Pravna osnova mora biti **dovoljno jasna** kako bi se građanima pružio odgovarajući uvid u uvjete i okolnosti u kojima su nadležna tijela ovlaštena primijeniti bilo kakve mjere prikupljanja podataka i tajnog nadzora. Pukim prenošenjem opće klauzule iz članka 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva u nacionalno pravo ne bi se postigla preciznost i predvidljivost.

Prije nego što nacionalni zakonodavac uspostavi novu pravnu osnovu za svaki oblik obrade biometrijskih podataka s pomoću prepoznavanja lica, treba provesti **savjetovanje** s nadležnim nadzornim tijelom za zaštitu podataka.

Zakonodavne mjere moraju biti **primjerene** za postizanje legitimnih ciljeva predmetnog zakonodavstva. **Cilj u općem interesu**, koliko god bio temeljan, sâm po sebi ne opravdava ograničenje temeljnog prava. Zakonodavne mjere trebale bi **razlikovati** i biti usmjerene na osobe koje su njima obuhvaćene s obzirom na cilj, kao što je borba protiv određenih teških kaznenih djela. Ako su mjerom

općenito obuhvaćene sve osobe bez takvog razlikovanja, ograničenja ili iznimke, njome se pojačava zadiranje u prava. Zadiranje u prava također se pojačava ako obrada podataka obuhvaća značajan dio stanovništva.

Podatci se moraju obrađivati na način kojim se jamče primjenjivost i učinkovitost pravilâ i načelâ EU-a o zaštiti podataka. **Procjenom nužnosti i proporcionalnosti** na temelju svake situacije također se moraju utvrditi i razmotriti sve moguće posljedice za druga temeljna prava. Ako se podatci sustavno obrađuju bez znanja ispitanikâ, vjerojatno će se stvoriti **opći osjećaj stalnog nadzora**. To može dovesti do odvraćajućih učinaka u pogledu nekih ili svih predmetnih temeljnih prava, kao što su ljudsko dostojanstvo iz članka 1. Povelje, sloboda mišljenja, savjesti i vjeroispovijedi iz članka 10. Povelje, sloboda izražavanja iz članka 11. Povelje te sloboda okupljanja i udruživanja iz članka 12. Povelje.

Obrada posebnih kategorija podataka, kao što su biometrijski podatci, može se smatrati „**nužnom**" (članak 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva) samo ako su zadiranje u zaštitu osobnih podataka i njegova ograničenja ograničeni na ono što je apsolutno nužno, tj. neophodno, pri čemu je isključena svaka obrada opće ili sustavne prirode.

Činjenica da je fotografiju **očito objavio ispitanik** (članak 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva) ne znači da se smatra da su očito objavljeni povezani biometrijski podatci, koji se mogu preuzeti s fotografije posebnim tehničkim sredstvima. Zadane postavke usluge, npr. stavljanje predložaka na raspolaganje javnosti ili nepostojanje mogućnosti izbora, npr. kada se predlošci objavljuju bez mogućnosti da korisnik promijeni tu postavku, ni na koji način ne bi trebalo tumačiti kao podatke koji su očito objavljeni.

Člankom 11. Direktive o zaštiti podataka pri izvršavanju zakonodavstva uspostavlja se okvir za **automatizirano pojedinačno donošenje odluka**. Upotreba tehnologije prepoznavanja lica podrazumijeva upotrebu posebnih kategorija podataka i može dovesti do izrade profila, ovisno o načinu i svrsi primjene tehnologije prepoznavanja lica. U svakom slučaju, u skladu s pravom Unije i člankom 11. stavkom 3. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, zabranjuje se izrada profila koja dovodi do diskriminacije pojedinaca na temelju posebnih kategorija osobnih podataka.

Članak 6. Direktive o zaštiti podataka pri izvršavanju zakonodavstva odnosi se na potrebu **razlikovanja između različitih kategorija ispitanika**. U pogledu ispitanika za koje ne postoje dokazi koji bi upućivali na to da bi njihovo ponašanje moglo imati poveznicu, čak i neizravnu ili udaljenu, s legitimnim ciljem u skladu s Direktivom o zaštiti podataka pri izvršavanju zakonodavstva, najvjerojatnije ne postoji opravdanje za zadiranje u prava.

Načelom smanjenja količine podataka (članak 4. stavak 1. točka (e) Direktive o zaštiti podataka pri izvršavanju zakonodavstva) također se propisuje da se svi videomaterijali koji nisu relevantni za svrhu obrade uvijek trebaju ukloniti ili anonimizirati (npr. zamagljivanjem bez retroaktivne mogućnosti povrata podataka) prije distribucije.

Voditelj obrade mora pažljivo razmotriti može li, i kako, ispuniti zahtjeve u pogledu **pravâ ispitanika** prije pokretanja bilo kakve obrade upotrebom tehnologije prepoznavanja lica jer ta tehnologija često uključuje obradu posebnih kategorija osobnih podataka bez ikakve očite interakcije s ispitanikom.

Učinkovito ostvarivanje prava ispitanika ovisi o tome ispunjava li voditelj obrade svoje **obveze informiranja** (članak 13. Direktive o zaštiti podataka pri izvršavanju zakonodavstva). Kada se procjenjuje postoji li „određeni slučaj" u skladu s člankom 13. stavkom 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, potrebno je uzeti u obzir nekoliko čimbenika, među ostalim i pitanje prikupljaju li se osobni podatci bez znanja ispitanika, jer bi to bio jedini način da se ispitanicima omogući

učinkovito ostvarivanje njihovih prava. Ako se donošenje odluka provodi isključivo na temelju tehnologije prepoznavanja lica, ispitanici moraju biti obaviješteni o značajkama automatiziranog donošenja odluka.

U pogledu **zahtjeva za pristup**, kada se biometrijski podatci pohranjuju i povezuju s identitetom s pomoću alfanumeričkih podataka, u skladu s načelom smanjenja količine podataka, nadležnom bi se tijelu trebalo omogućiti da potvrdi zahtjev za pristup na temelju pretraživanja tih alfanumeričkih podataka bez pokretanja daljnje obrade biometrijskih podataka drugih osoba (tj. pretraživanjem baze podataka primjenom tehnologije prepoznavanja lica).

Rizici za ispitanike osobito su ozbiljni ako se netočni podatci pohranjuju u policijskoj bazi podataka i/ili se razmjenjuju s drugim subjektima. Voditelj obrade mora u skladu s time **ispraviti** pohranjene podatke i sustave tehnologije prepoznavanja lica (vidjeti također uvodnu izjavu 47. Direktive o zaštiti podataka pri izvršavanju zakonodavstva).

Pravo na **ograničenje** postaje osobito važno kada se radi o tehnologiji prepoznavanja lica (na temelju jednog ili više algoritama, što znači da se nikad ne prikazuje konačan rezultat) u situacijama u kojima se prikupljaju velike količine podataka te može doći do odstupanja u pogledu točnosti i kvalitete identifikacije.

Procjena učinka na zaštitu podataka prije upotrebe tehnologije prepoznavanja lica obvezni je zahtjev, usp. članak 27. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. Europski odbor za zaštitu podataka (EDPB) preporučuje objavljivanje rezultata takvih procjena ili barem glavnih nalaza i zaključaka procjene učinka na zaštitu podataka kao mjeru za jačanje povjerenja i transparentnosti.

Većina slučajeva uvođenja i upotrebe tehnologije prepoznavanja lica predstavlja intrinzično visok rizik za prava i slobode ispitanikâ. Stoga bi se nadležno tijelo koje uvodi tehnologiju prepoznavanja lica trebalo **savjetovati** s nadležnim nadzornim tijelom prije uvođenja sustava.

S obzirom na jedinstvenu prirodu biometrijskih podataka, tijelo koje provodi i/ili upotrebljava tehnologiju prepoznavanja lica trebalo bi posvetiti osobitu pozornost **sigurnosti obrade**, u skladu s člankom 29. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. Konkretno bi tijelo za izvršavanje zakonodavstva trebalo osigurati usklađenost sustava s relevantnim normama i provoditi mjere za zaštitu biometrijskih predložaka. Načela i postupovna jamstva u pogledu zaštite podataka moraju biti ugrađeni u tehnologiju prije početka obrade osobnih podataka. Prema tome, čak i ako tijelo za izvršavanje zakonodavstva namjerava primjenjivati i upotrebljavati tehnologiju prepoznavanja lica od vanjskih pružatelja usluga, mora, primjerice, putem postupka nabave osigurati da se primjenjuje samo tehnologija prepoznavanja lica koja se temelji na **načelima tehničke i integrirane zaštite podataka**.

Zapisivanje (usp. članak 25. Direktive o zaštiti podataka pri izvršavanju zakonodavstva) važno je postupovno jamstvo za provjeru zakonitosti obrade interno (samopraćenje predmetnog voditelja obrade/izvršitelja obrade) te na raspolaganju vanjskim nadzornim tijelima. U kontekstu sustavâ za prepoznavanje lica, zapisivanje se također preporučuje za promjene referentne baze podataka i za pokušaje identifikacije ili provjere, uključujući korisnika, ishod i ocjenu pouzdanosti. Međutim, zapisivanje je samo jedan od ključnih elemenata sveobuhvatnog **načela odgovornosti** (usp. članak 4. stavak 4. Direktive o zaštiti podataka pri izvršavanju zakonodavstva). Voditelj obrade mora moći dokazati usklađenost obrade s osnovnim načelima zaštite podataka iz članka 4. stavaka od 1. do 3. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

EDPB podsjeća da je zajedno s EDPS-om objavio **poziv na zabranu** određenih vrsta obrade u vezi s 1. daljinskom biometrijskom identifikacijom pojedinaca na javno dostupnim mjestima; 2. sustavima prepoznavanja lica na temelju umjetne inteligencije kojima se pojedinci na temelju biometrijskih podataka kategoriziraju u skupine prema etničkoj pripadnosti, rodu, kao i političkoj ili seksualnoj orijentaciji ili drugim osnovama za diskriminaciju; 3. upotrebom tehnologije prepoznavanja lica ili sličnih tehnologija za izvođenje zaključaka o emocijama pojedinaca; i 4. obradom osobnih podataka u kontekstu izvršavanja zakonodavstva koja bi se temeljila na bazi podataka popunjenoj masovno i neselektivno prikupljenim osobnim podatcima, npr. „struganjem ekrana" za ekstrakciju fotografija i prikaza lica dostupnih na internetu.

Središnja mjera za zaštitu temeljnih prava o kojima je riječ jest **učinkovit nadzor** nadležnih nadzornih tijela za zaštitu podataka. Stoga države članice moraju osigurati da su resursi nadzornih tijela primjereni i dostatni kako bi im se omogućilo da izvršavaju svoje ovlasti.

Ove su **smjernice upućene** donositeljima zakona na razini EU-a i nacionalnoj razini, kao i tijelima za izvršavanje zakonodavstva i njihovima službenicima koji provode i upotrebljavaju sustave tehnologije prepoznavanja lica. Pojedincima su upućene u mjeri u kojoj su općenito zainteresirani ili u svojstvu ispitanika, osobito u pogledu prava ispitanika.

Svrha ovih smjernica jest pružiti informacije o određenim svojstvima tehnologije prepoznavanja lica i primjenjivom pravnom okviru u kontekstu izvršavanja zakonodavstva (posebno Direktive o zaštiti podataka pri izvršavanju zakonodavstva).

- Osim toga, služe kao **alat za podršku prvoj klasifikaciji osjetljivosti određenog slučaja upotrebe** (Prilog I.).
- Također sadrže **praktične smjernice za tijela za izvršavanje zakonodavstva koja žele nabaviti i primjenjivati sustav tehnologije prepoznavanja lica** (Prilog II.).
- U Smjernicama je također prikazano nekoliko tipičnih **slučajeva upotrebe te su navedena brojna relevantna razmatranja**, osobito u pogledu ispitivanja nužnosti i proporcionalnosti (Prilog III.).

1 UVOD

1. Tehnologija prepoznavanja lica može se upotrebljavati za automatsko prepoznavanje pojedinaca na temelju njihova lica. Tehnologija prepoznavanja lica često se temelji na umjetnoj inteligenciji, kao što su tehnologije strojnog učenja. Primjene tehnologije prepoznavanja lica sve se više ispituju i upotrebljavaju u različitim područjima, od pojedinačne upotrebe do upotrebe u privatnim organizacijama i javnoj upravi. Tijela za izvršavanje zakonodavstva također očekuju da će ostvariti koristi od primjene tehnologije prepoznavanja lica. Očekuje se da će ta tehnologija pružiti rješenja za relativno nove izazove, kao što su istrage koje uključuju veliku količinu prikupljenih dokaza, ali i za poznate probleme, osobito u pogledu nedovoljnog broja osoblja za obavljanje zadataka promatranja i pretraživanja.

2. Povećani interes za tehnologiju prepoznavanja lica uvelike se temelji na učinkovitosti i prilagodljivosti tehnologije prepoznavanja lica. To je popraćeno nedostatcima svojstvenima tehnologiji i njezinoj primjeni, također u velikim razmjerima. Iako se pritiskom gumba može analizirati na tisuće skupova osobnih podataka, već blagi učinci algoritamske diskriminacije ili pogrešne identifikacije mogu značajno pogoditi veliki broj pojedinaca u smislu njihova ponašanja i svakodnevnog života. Sam opseg obrade osobnih podataka, te osobito biometrijskih podataka, dodatni je ključni element tehnologije

prepoznavanja lica jer obrada osobnih podataka predstavlja zadiranje u temeljno pravo na zaštitu osobnih podataka u skladu s člankom 8. Povelje Europske unije o temeljnim pravima (Povelja).

3. Tehnologije prepoznavanja lica koje primjenjuju tijelâ za izvršavanje zakonodavstva imat će (a u određenoj mjeri već ima) značajne posljedice na pojedince i skupine ljudi, uključujući manjine. Te će posljedice imati značajne učinke na način zajedničkog života te na našu društvenu i demokratsku političku stabilnost, uzimajući u obzir značaj pluralizma i političke oporbe. Pravo na zaštitu osobnih podataka često je nužan preduvjet za jamstvo drugih temeljnih prava. Primjena tehnologije prepoznavanja lica u znatnoj je mjeri sklona zadiranju u temeljna prava povrh prava na zaštitu osobnih podataka.

4. EDPB stoga smatra da je važno doprinijeti aktualnoj integraciji tehnologije prepoznavanja lica u području izvršavanja zakonodavstva obuhvaćene Direktivom o zaštiti podataka pri izvršavanju zakonodavstva[1], odnosno nacionalnim zakonima kojima se ona prenosi, te da je važno izdati ove Smjernice. Svrha ovih Smjernica jest pružiti relevantne informacije donositeljima zakona na razini EU-a i na nacionalnoj razini, kao i tijelima za izvršavanje zakonodavstva i njihovim službenicima pri provedbi i uporabi sustava tehnologije prepoznavanja lica. Područje primjene Smjernica ograničeno je na tehnologiju prepoznavanja lica. Međutim, drugi oblici obrade osobnih podataka koju provode tijela za izvršavanje zakonodavstva na temelju biometrijskih podataka, osobito ako se obrađuju na daljinu, mogu predstavljati slične ili dodatne rizike za pojedince, skupine i društvo. U skladu s odgovarajućim okolnostima, neki aspekti ovih Smjernica također mogu poslužiti kao koristan izvor u tim slučajevima. Konačno, pojedinci zainteresirani općenito ili u svojstvu ispitanika također mogu pronaći važne informacije, osobito u pogledu prava ispitanika.

5. Smjernice se sastoje od glavnog dokumenta i triju priloga. U glavnom dokumentu predstavljeni su tehnologija i primjenjivi pravni okvir. Kako bi se lakše utvrdili neki od glavnih aspekata za klasifikaciju težine zadiranja u temeljna prava u određenom području primjene, u Prilogu I. dostupan je predložak. Tijela za izvršavanje zakonodavstva koja žele nabaviti i primjenjivati sustav tehnologije prepoznavanja lica mogu pronaći praktične smjernice u Prilogu II. Ovisno o području primjene tehnologije prepoznavanja lica, mogu biti relevantna različita razmatranja. U Prilogu III. naveden je skup hipotetskih scenarija i relevantnih razmatranja.

2 TEHNOLOGIJA

2.1 Jedna biometrijska tehnologija, dvije različite funkcije

6. Prepoznavanje lica probabilistička je tehnologija koja može automatski prepoznati pojedince na temelju njihova lica u svrhu njihove autentifikacije ili identifikacije.

7. Tehnologija prepoznavanja lica dio je šire kategorije biometrijske tehnologije. Biometrijski podatci uključuju sve automatizirane postupke koji se upotrebljavaju za prepoznavanje pojedinca kvantificiranjem fizičkih obilježja, fizioloških obilježja ili obilježja ponašanja (otisci prstiju, struktura šarenice, glas, hod, uzorci krvnih žila itd.). Ta su obilježja definirana kao „biometrijski podatci” jer omogućuju ili potvrđuju jedinstvenu identifikaciju te osobe.

[1] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.

8. To je slučaj s licima ljudi ili, konkretnije, s njihovom tehničkom obradom s pomoću uređaja za prepoznavanje lica: na temelju prikaza lica (snimanjem fotografije ili videozapisa), koji se naziva biometrijskim „uzorkom", moguće je izdvojiti digitalni prikaz različitih obilježja tog lica (što se naziva „predloškom").

9. Biometrijski predložak digitalni je prikaz jedinstvenih značajki izdvojenih iz biometrijskog uzorka, koje se mogu pohraniti u biometrijskoj bazi podataka[2]. Ovaj predložak trebao bi biti jedinstven i specifičan za svaku osobu te je u načelu stalan tijekom vremena[3]. U fazi prepoznavanja uređaj uspoređuje ovaj predložak s drugim predlošcima koji su prethodno proizvedeni ili izračunati izravno iz biometrijskih uzoraka, kao što su lica pronađena na prikazu, fotografiji ili videozapisu. Prema tome, „prepoznavanje lica" postupak je u dva koraka: prikupljanje prikaza lica i njegova pretvorba u predložak, nakon čega slijedi prepoznavanje lica usporedbom odgovarajućeg predloška s jednim ili više drugih predložaka.

10. Kao i svaki biometrijski postupak, prepoznavanje lica može imati dvije različite svrhe:

- **autentifikaciju** osobe, čiji je cilj provjeriti je li osoba ona za koju tvrdi da jest. U tom će slučaju sustav usporediti prethodno snimljeni biometrijski predložak ili uzorak (pohranjen na pametnoj kartici ili biometrijskoj putovnici) s jednim licem, kao što je lice osobe koja se pojavljuje na kontrolnoj točki, kako bi se provjerilo je li riječ o jednoj te istoj osobi. Stoga se ta funkcija oslanja na usporedbu dvaju predložaka. To se također naziva **provjerom** usporedbom dvaju uzoraka

- **identifikaciju** osobe, s ciljem pronalaska osobe među skupinom pojedinaca unutar određenog područja, slike ili baze podataka. U tom slučaju sustav mora obraditi sva snimljena lice kako bi generirao biometrijski predložak, a zatim provjeriti podudara li se s osobom koja je poznata sustavu. Ta se funkcija stoga oslanja na usporedbu jednog predloška s bazom predložaka ili uzoraka (polazište). To se također naziva identifikacijom usporedbom više uzoraka. Primjerice, na taj se način zapis osobnog imena (prezime, ime) može povezati s licem ako se usporedba vrši u odnosu na bazu podataka fotografija povezanih s prezimenima i imenima. Također može uključivati praćenje osobe kroz skupinu ljudi, pri čemu se ne mora nužno uspostaviti veza s njezinim građanskim identitetom.

11. U oba se slučaja upotrijebljene tehnike prepoznavanja lica temelje na procijenjenoj podudarnosti između predložaka: predloška koji se uspoređuje i polazišta. U tom su smislu tehnike probabilističke: iz usporedbe proizlazi veća ili manja vjerojatnost da je osoba zaista osoba koju treba autentificirati ili identificirati. Ako ta vjerojatnost premašuje određeni prag u sustavu koji je definirao korisnik ili razvojni programer sustava, sustav će pretpostaviti da postoji podudaranje.

12. Iako se te funkcije, autentifikacija i identifikacija, razlikuju, obje se odnose na obradu biometrijskih podataka koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi te stoga predstavljaju obradu osobnih podataka, točnije obradu posebnih kategorija osobnih podataka.

13. Prepoznavanje lica dio je šireg spektra tehnika obrade videozapisa. Neke videokamere mogu snimati ljude u određenom području, posebno njihova lica, ali se kao takve ne mogu upotrebljavati za automatsko prepoznavanje pojedinaca. Isto vrijedi i za jednostavnu fotografiju: kamera nije sustav prepoznavanja lica jer se fotografije ljudi moraju obrađivati na poseban način kako bi se prikupili biometrijski podatci.

[2] Smjernice o prepoznavanju lica, Savjetodavni odbor Konvencije 108, Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka, Vijeće Europe, lipanj 2021.

[3] To može ovisiti o vrsti biometrije i dobi ispitanika.

14. Nadalje, detekcija lica s pomoću takozvanih „pametnih” kamera ne predstavlja nužno sustav prepoznavanja lica. Iako njihova primjena otvara važna pitanja u pogledu etike i djelotvornosti, digitalnih tehnika za otkrivanje neuobičajenog ponašanja, nasilnih događaja ili za prepoznavanje emocija na licima ili čak silueta, ne mogu se smatrati biometrijskim sustavima koji obrađuju posebne kategorije osobnih podataka, pod uvjetom da nisu usmjereni na jedinstvenu identifikaciju osobe i da uključena obrada osobnih podataka ne obuhvaća druge posebne kategorije osobnih podataka. Ti primjeri nisu potpuno nepovezani s prepoznavanjem lica i još uvijek podliježu pravilima o zaštiti osobnih podataka.[4] Nadalje, ta vrsta sustava za otkrivanje može se upotrebljavati zajedno s drugim sustavima čiji je cilj identifikacija osobe, zbog čega se smatra tehnologijom prepoznavanja lica.

15. Za razliku od sustavâ za snimanje i obradu videozapisa, koji zahtijevaju postavljanje fizičkih uređaja, prepoznavanje lica softverska je funkcija koja se može primijeniti u okviru postojećih sustava (kamere, baze podataka slika itd.). Stoga takva funkcija može biti povezana ili u sučelju s mnoštvom sustava te se može kombinirati s drugim funkcijama. Takva integracija u već postojeću infrastrukturu zahtijeva osobitu pozornost jer podrazumijeva inherentne rizike koji nastaju zbog činjenice da bi tehnologija prepoznavanja lica mogla biti neprimjetna i lako skrivena[5].

2.2 Širok raspon svrha i primjena

16. Izvan područja primjene ovih Smjernica i izvan područja primjene Direktive o zaštiti podataka pri izvršavanju zakonodavstva, prepoznavanje lica može se upotrebljavati za širok raspon ciljeva, kako za komercijalnu uporabu, tako i za rješavanje pitanja javne sigurnosti ili izvršavanja zakonodavstva. Može se primjenjivati u različitim kontekstima: u osobnom odnosu između korisnika i usluge (pristup aplikaciji), za pristup određenom mjestu (fizičko filtriranje) ili bez ikakvih posebnih ograničenja u javnom prostoru (prepoznavanje lica u stvarnom vremenu). Može se primjenjivati na bilo koju vrstu ispitanika: na korisnika usluge, zaposlenika, promatrača, traženu osobu ili osobu povezanu s pravnim ili upravnim postupkom itd. Neke su uporabe već uobičajene i raširene, dok su druge trenutačno u eksperimentalnoj ili špekulativnoj fazi. Iako se ove Smjernice neće odnositi na sve takve uporabe i primjene, EDPB podsjeća da se mogu provoditi samo ako su u skladu s primjenjivim pravnim okvirom, osobito s OUZP-om i relevantnim nacionalnim zakonima.[6] Čak i u kontekstu Direktive o zaštiti podataka pri izvršavanju zakonodavstva, osim za funkcije autentifikacije ili identifikacije, podatci koji se obrađuju s pomoću tehnologije prepoznavanja lica mogu se dodatno obrađivati u druge svrhe, kao što je kategorizacija.

17. Konkretno se može razmotriti opseg mogućih uporaba ovisno o stupnju kontrole koju ljudi imaju nad svojim osobnim podatcima, o učinkovitim sredstvima koja su im dostupna za izvršavanje takve kontrole i o njihovu pravu na inicijativu pokretanja i upotrebe te tehnologije, posljedicama za njih (u slučaju prepoznavanja ili neprepoznavanja) te opsegu provedene obrade. Prepoznavanje lica na temelju predloška pohranjenog na osobnom uređaju (pametna kartica, pametni telefon itd.) koji pripada toj osobi i upotrebljava se za autentifikaciju i strogo osobne uporabe putem namjenskog sučelja, ne predstavlja iste rizike kao, primjerice, upotreba za potrebe identifikacije u nekontroliranom okruženju, bez aktivnog sudjelovanja ispitanika, pri čemu se predložak svakog lica koje ulazi u područje praćenja uspoređuje s predlošcima iz širokog poprečnog presjeka stanovništva pohranjenima u bazi podataka.

[4] Međutim, članak 10. Direktive o izvršavanju zakonodavstva (ili članak 9. OUZP-a) primjenjiv je na sustave koji se upotrebljavaju za kategorizaciju pojedinaca na temelju njihovih biometrijskih podataka u klastere prema etničkom podrijetlu, kao i političkoj ili seksualnoj orijentaciji ili drugim posebnim kategorijama osobnih podataka.
[5] Primjerice, u kamerama koje se nose na tijelu i koje se sve više upotrebljavaju u praksi.
[6] Za dodatne smjernice vidjeti također Smjernice EDPB-a br. 3/2019 o obradi osobnih podataka putem videouređaja donesene 29. siječnja 2020.

Između tih dviju krajnosti nalazi se vrlo različit spektar upotreba i povezanih pitanja koja se odnose na zaštitu osobnih podataka.

18. Kako bi se dodatno ilustrirao kontekst u kojem se trenutačno raspravlja o tehnologijama prepoznavanja lica ili se te tehnologije primjenjuju u svrhu autentifikacije ili identifikacije, EDPB smatra važnim navesti niz primjera. Primjeri u nastavku samo su opisni i ne bi ih trebalo smatrati preliminarnom procjenom njihove usklađenosti s pravnom stečevinom EU-a u području zaštite podataka.

Primjeri autentifikacije s pomoću tehnologije prepoznavanja lica

19. Autentifikacija može biti osmišljena na način da korisnici imaju potpunu kontrolu nad njom, primjerice, kako bi se omogućio pristup uslugama ili aplikacijama isključivo u kućnom okruženju. Stoga vlasnici pametnih telefona u velikoj mjeri upotrebljavaju tu funkciju za otključavanje svojeg uređaja, umjesto autentifikacije s pomoću lozinke.

20. Autentifikacija s pomoću prepoznavanja lica također se može upotrebljavati za provjeru identiteta osobe koja želi ostvariti koristi od javnih ili privatnih usluga trećih strana. Stoga takvi postupci nude način stvaranja digitalnog identiteta putem mobilne aplikacije (pametni telefon, tablet-računalo itd.), koji se zatim može upotrebljavati za pristup administrativnim uslugama na internetu.

21. Nadalje, autentifikacija s pomoću prepoznavanja lica može biti usmjerena na kontrolu fizičkog pristupa jednoj ili više unaprijed određenih lokacija, kao što su ulazi u zgrade ili posebni granični prijelazi. Primjerice, ta se funkcija primjenjuje u određenim postupcima obrade u svrhu prelaska granice, pri čemu se lice osobe na uređaju kontrolne točke uspoređuju s prikazom lica pohranjenim u njezinoj identifikacijskoj ispravi (putovnica ili sigurna boravišna dozvola).

Primjeri identifikacije s pomoću tehnologije prepoznavanja lica

22. Identifikacija se može primjenjivati na brojne, izrazito raznolike načine. To osobito uključuje, ali nije ograničeno na, upotrebe navedene u nastavku, koje su trenutačno predmet promatranja, pokusa ili planiranja u EU-u:

- pretraživanje identiteta neidentificirane osobe (žrtve, osumnjičenika itd.) u bazi podataka koja sadrži fotografije
- nadzor nad kretanjem osobe u javnom prostoru. Lice osobe uspoređuje se s biometrijskim predlošcima osoba koje putuju ili su putovale u nadziranom području, primjerice, kada je ostavljen komad prtljage ili nakon počinjenja kaznenog djela
- rekonstruiranje putovanja osobe i njezinih naknadnih interakcija s drugim osobama putem odgođene usporedbe istih elemenata u nastojanju da se, primjerice, utvrde njihovi kontakti
- daljinsku biometrijsku identifikaciju traženih osoba u javnim prostorima. Sva lica snimljena videokamerama u stvarnom vremenu simultano se unakrsno se provjeravaju usporedbom s bazom podataka sigurnosnih snaga
- automatsko prepoznavanje ljudi prikazanih na slici kako bi se, primjerice, identificirali njihovi odnosi na društvenoj mreži koja se njome koristi. Slika se uspoređuje s predlošcima svih korisnika mreže koji su prihvatili tu funkciju kako bi se predložila načelna identifikacija tih odnosa
- pristup uslugama, pri čemu neki uređaji za isplatu gotovine prepoznaju svoje klijente, uspoređivanjem prikaza lica snimljenog kamerom s bazom podataka prikaza lica koju vodi banka

- praćenje putovanja putnika u određenoj fazi putovanja. Predložak, izračunat u stvarnom vremenu, za svaku osobu koja se prijavljuje na lokacijama koje se nalaze u određenim fazama putovanja (točke za predaju prtljage, vrata za ukrcaj itd.), uspoređuje se s predlošcima osoba koje su prethodno registrirane u sustavu.

23. Osim primjene tehnologije prepoznavanja lica u području izvršavanja zakonodavstva, širok raspon zabilježenih primjena svakako zahtijeva sveobuhvatnu raspravu i politički pristup kako bi se osigurala dosljednost i usklađenost s pravnom stečevinom EU-a u području zaštite podataka.

2.3 Pouzdanost, točnost i rizici za ispitanike

24. Kao što je slučaj sa svim tehnologijama, u pogledu prepoznavanja lica može doći do izazova u provedbi, osobito kad je riječ o pouzdanosti i učinkovitosti u pogledu autentifikacije ili identifikacije, kao i o cjelokupnom pitanju kvalitete i točnosti „izvornih" podataka i rezultata obrade na temelju tehnologije prepoznavanja lica.

25. Takvi tehnološki izazovi podrazumijevaju posebne rizike za predmetne ispitanike, koji su utoliko značajniji ili ozbiljniji u području izvršavanja zakonodavstva zbog mogućih pravnih ili sličnih učinaka na ispitanike. U tom se kontekstu također čini korisnim naglasiti da ex post upotreba tehnologije prepoznavanja lica sama po sebi nije sigurnija jer se pojedinci mogu pratiti u vremenu i mjestima. Stoga ex post upotreba također predstavlja posebne rizike, koje je potrebno procijeniti od slučaja do slučaja.[7]

26. Kao što je Agencija EU-a za temeljna prava istaknula u svojem izvješću iz 2019., „utvrđivanje potrebne razine točnosti softvera za prepoznavanje lica komplicirano je: postoji mnogo različitih načina ocjenjivanja i procjene točnosti, među ostalim ovisno o zadaći, svrsi i kontekstu upotrebe. Kada se tehnologija primjenjuje na mjestima koja posjećuju milijuni ljudi, kao što su željezničke stanice ili zračne luke, relativno mali udio pogrešaka (npr. 0,01 %)[8] i dalje podrazumijeva da su stotine ljudi pogrešno označene. Osim toga, vjerojatnije je da će se za određene kategorije osoba dobiti pogrešno podudaranje, kako je opisano u odjeljku 3. Budući da postoje različiti načini izračuna i tumačenja stopa pogreške, potreban je oprez. Osim toga, u pogledu točnosti i pogrešaka, pitanja o tome koliko se lako sustav može prevariti, na primjer, lažnim prikazima lica (što se naziva imitacijom), važna su posebno za potrebe izvršavanja zakonodavstva."[9]

27. U tom kontekstu EDPB smatra važnim podsjetiti da tehnologija prepoznavanja lica, bez obzira na to upotrebljava li se za potrebe autentifikacije ili identifikacije, ne nudi konačan rezultat, već se oslanja na vjerojatnosti da dva lica ili prikaza lica odgovaraju istoj osobi.[10] Taj se rezultat dodatno pogoršava kada je kvaliteta unosa biometrijskih uzoraka u svrhu prepoznavanja lica niska. Zamućenost ulaznih prikaza, niska razlučivost kamere, pokret i niska razina svjetlosti mogu biti čimbenici koji doprinose niskoj kvaliteti. Drugi aspekti koji značajno utječu na rezultate jesu učestalost i zavaravanje, npr. kada kriminalci nastoje izbjeći prolazak pored kamera ili prevariti tehnologiju prepoznavanja lica. U brojnim je studijama također istaknuto da takvi statistički rezultati algoritamske obrade također mogu biti podložni predrasudama, što osobito proizlazi iz kvalitete izvornih podataka, kao i baza podataka za uvježbavanje ili drugih čimbenika, kao što je odabir lokacije za uvođenje tehnologije. Nadalje, također bi trebalo istaknuti utjecaj tehnologije prepoznavanja lica na druga temeljna prava, kao što su

[7] Vidjeti primjere navedene u Prilogu III.
[8] Ta stopa točnosti proizlazi iz citiranog izvješća i odražava stopu znatno bolju od trenutačne stope učinkovitosti algoritama u primjenama tehnologije prepoznavanja lica.
[9] Tehnologija prepoznavanja lica: pitanje temeljnih prava u kontekstu izvršavanja zakonodavstva, Agencija Europske unije za temeljna prava, 21. studenoga 2019.
[10] Ta se vjerojatnost naziva „ocjenom pouzdanosti".

poštovanje privatnog i obiteljskog života, sloboda izražavanja i informiranja, sloboda okupljanja i udruživanja itd.

28. Stoga je ključno da se pouzdanost i točnost tehnologije prepoznavanja lica uzmu u obzir kao kriteriji za procjenu usklađenosti s ključnim načelima zaštite podataka, u skladu s člankom 4. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, osobito kada je riječ o pravednosti i točnosti.

29. Iako ističe da su za kvalitetne algoritme presudni kvalitetni podatci, EDPB također naglašava potrebu za time da voditelji obrade podataka u okviru svoje obveze odgovornosti provode redovitu i sustavnu procjenu algoritamske obrade, osobito kako bi se osigurala točnost, pravednost i pouzdanost rezultata takve obrade osobnih podataka. Osobni podatci koji se upotrebljavaju za potrebe provjere, uvježbavanja i daljnjeg razvoja sustava tehnologije prepoznavanja lica smiju se obrađivati samo na temelju dostatne pravne osnove i u skladu sa zajedničkim načelima zaštite podataka.

3 MJERODAVAN PRAVNI OKVIR:

30. Upotreba tehnologija prepoznavanja lica neodvojivo je povezana s obradom osobnih podataka, uključujući posebne kategorije podataka. Osim toga, izravno ili neizravno utječe na niz temeljnih prava utvrđenih u Povelji EU-a o temeljnim pravima. To je osobito važno u području izvršavanja zakonodavstva i kaznenog pravosuđa. Stoga bi se svaka upotreba tehnologija prepoznavanja lica trebala provoditi u skladu s primjenjivim pravnim okvirom.

31. Informacije navedene u nastavku trebale bi se upotrebljavati za razmatranje pri ocjenjivanju budućih zakonodavnih i administrativnih mjera, kao i pri provedbi postojećeg zakonodavstva na osnovi pojedinačnog slučaja koji obuhvaća tehnologiju prepoznavanja lica. Relevantnost zahtjevâ razlikuje se ovisno o konkretnim okolnostima. Budući da se ne mogu predvidjeti sve buduće okolnosti, primjeri u nastavku smatraju se samo doprinosom te se ne smiju tumačiti kao iscrpan popis.

3.1 Opći pravni okvir – Povelja EU-a o temeljnim pravima i Europska konvencija o ljudskim pravima

3.1.1 Primjenjivost Povelje

32. Povelja EU-a o temeljnim pravima (u daljnjem tekstu: Povelja) upućena je institucijama, tijelima, uredima i agencijama Unije te državama članicama prilikom provedbe prava Europske unije.

33. Reguliranjem obrade biometrijskih podataka za potrebe izvršavanja zakonodavstva u skladu s člankom 1. stavkom 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva neizbježno se postavlja pitanje usklađenosti s temeljnim pravima, posebno poštovanjem privatnog života i komuniciranja u skladu s člankom 7. Povelje i pravom na zaštitu osobnih podataka u skladu s člankom 8. Povelje.

34. Prikupljanje i analiza videozapisa fizičkih osoba, uključujući njihovih lica, podrazumijeva obradu osobnih podataka. Kada se radi o tehničkoj obradi slike, obrada također obuhvaća biometrijske podatke. Tehnička obrada podataka koji se odnose na lice fizičke osobe u odnosu na vrijeme i mjesto omogućuje donošenje zaključaka o privatnom životu relevantnih osoba. Ti se zaključci mogu odnositi na rasno ili etničko podrijetlo, zdravlje, vjeru, navike u svakodnevnom životu, trajna ili privremena mjesta boravka, svakodnevna ili druga kretanja, aktivnosti koje se obavljaju, društvene odnose tih osoba i društveno okruženje u kojem se te osobe nalaze. Široki raspon informacija koje se mogu otkriti

primjenom tehnologije prepoznavanja lica jasno ukazuje na mogući utjecaj na pravo na zaštitu osobnih podataka utvrđeno u članku 8. Povelje, ali i na pravo na privatnost utvrđeno u članku 7. Povelje.

35. U takvim okolnostima također nije nezamislivo da bi prikupljanje, analiza i daljnja obrada predmetnih biometrijskih podataka (na temelju prikaza lica) mogla utjecati na način na koji se ljudi osjećaju slobodnima djelovati, čak i ako bi to djelovanje bilo u potpunosti u okviru slobodnog i otvorenog društva. To bi također moglo imati ozbiljne posljedice na ostvarivanje njihovih temeljnih prava, kao što su njihovo pravo na slobodu mišljenja, savjesti i vjeroispovijedi, na slobodu mirnog okupljanja i slobodu udruživanja u skladu s člancima 1., 10., 11. i 12. Povelje. Takva obrada uključuje i druge rizike, kao što je rizik od zlouporabe osobnih informacija koje su prikupila nadležna tijela kao rezultat nezakonitog pristupa osobnim podatcima i njihove uporabe, povrede sigurnosti i sl. Rizici često ovise o obradi i njezinim okolnostima, kao što je rizik da policijski službenici ili druge neovlaštene strane nezakonito pristupe podatcima ili ih koriste. Međutim, neki su rizici svojstveni jedinstvenoj prirodi biometrijskih podataka. Za razliku od adrese ili telefonskog broja, ispitanik ne može promijeniti svoja jedinstvena obilježja, kao što su lice ili šarenica. U slučaju neovlaštenog pristupa ili slučajnog objavljivanja biometrijskih podataka, to bi dovelo do ugrožavanja upotrebe podataka u svojstvu lozinki ili kriptografskih ključeva ili bi se ti podatci mogli upotrijebiti za daljnje, neovlaštene aktivnosti nadzora na štetu ispitanika.

3.1.2 Zadiranje u prava utvrđena Poveljom

36. Obrada biometrijskih podataka u svim okolnostima sama po sebi predstavlja teško zadiranje u prava. To ne ovisi o ishodu, npr. pronalasku podudaranja. Obrada predstavlja zadiranje u prava čak i ako se biometrijski predložak odmah izbriše nakon što se usporedbom s policijskom bazom podataka ne dobije rezultat.

37. Zadiranje u temeljna prava ispitanikâ može proizlaziti iz pravnog akta čiji je cilj ili učinak ograničavanje odnosnog temeljnog prava[11]. Također može proizaći iz čina tijela javne vlasti s istom svrhom ili učinkom ili čak iz čina privatnog subjekta kojemu je zakonom povjereno izvršavanje javne vlasti i javnih ovlasti.

38. Zakonodavna mjera koja služi kao pravna osnova za obradu osobnih podataka izravno utječe na prava zajamčena člancima 7. i 8. Povelje[12].

39. Upotreba biometrijskih podataka te osobito tehnologije prepoznavanja lica u mnogim slučajevima također utječe na pravo na ljudsko dostojanstvo, zajamčeno člankom 1. Povelje. Ljudsko dostojanstvo zahtijeva da se prema pojedincima ne postupa kao prema predmetima. Tehnologija prepoznavanja lica pretvara egzistencijalna i vrlo osobna obilježja, obilježja lica, u strojno čitljiv oblik u svrhu njegove upotrebe u svojstvu ljudske registarske pločice ili osobne iskaznice, čime se lice objektivizira.

40. Takva obrada može zadirati i u druga temeljna prava, kao što su prava iz članaka 10., 11. i 12. Povelje, u mjeri u kojoj su odvraćajući učinci predviđeni relevantnim videonadzorom agencija za izvršavanje zakonodavstva ili proizlaze iz njega.

41. Osim toga, također bi trebalo pažljivo razmotriti moguće rizike koji nastaju zbog upotrebe tehnologija prepoznavanja lica koje provode tijela za izvršavanje zakonodavstva u pogledu prava na pošteno suđenje i pretpostavke nedužnosti u skladu s člancima 47. i 48. Povelje. Rezultat primjene tehnologije prepoznavanja lica, npr. podudaranje, ne samo da može dovesti do podvrgavanja osobe daljnjem policijskom nadzoru, nego također može predstavljati odlučujući dokaz u sudskim postupcima. Stoga

[11] Sud EU-a, C-219/91 – Ter Voort, RoC 1992 I-05485, t. 36.f.; Sud EU-a, C-200/96 – Metronome, RoC 1998 I-1953, t. 28.

[12] Sud EU-a, C-594/12, t. 36.; Sud EU-a, C-291/12, t. 23. i sljedeće.

nedostatci tehnologije prepoznavanja lica, kao što su moguća pristranost, diskriminacija ili pogrešna identifikacija („lažno pozitivan rezultat”), mogu dovesti do ozbiljnih posljedica u pogledu kaznenih postupaka. Nadalje, u ocjeni dokaza može se dati prednost ishodu primjene tehnologije prepoznavanja lica, čak i ako postoje proturječni dokazi („automatska pristranost”).

3.1.3 Opravdanje za zadiranje u prava

42. U skladu s člankom 52. stavkom 1. Povelje, svako ograničenje pri ostvarivanju prava i sloboda mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Europska unija ili potrebi zaštite prava i sloboda drugih osoba.

3.1.3.1 Predviđeno zakonom

43. U članku 52. stavku 1. Povelje utvrđuje se zahtjev posebne pravne osnove. Ta pravna osnova mora biti dovoljno jasna kako bi se građanima pružile odgovarajuće informacije o uvjetima i okolnostima u kojima su nadležna tijela ovlaštena primijeniti bilo kakve mjere prikupljanja podataka i tajnog nadzora[13]. Podrazumijeva da je nužno s razumnom jasnoćom navesti opseg i način izvršavanja relevantnog diskrecijskog prava dodijeljenog javnim tijelima kako bi se pojedincima osigurao minimalni stupanj zaštite u skladu s vladavinom prava u demokratskom društvu[14]. Osim toga, zakonitost zahtijeva odgovarajuća postupovna jamstva kako bi se posebno osiguralo poštovanje prava pojedinca iz članka 8. Povelje. Ta se načela također primjenjuju na obradu osobnih podataka u svrhu procjene, uvježbavanja i daljnjeg razvoja sustavâ tehnologije prepoznavanja lica.

44. S obzirom na činjenicu da biometrijski podatci koji se obrađuju u svrhu jedinstvene identifikacije pojedinca čine posebne kategorije podataka navedene u članku 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, za različite primjene tehnologije prepoznavanja lica u većini bi slučajeva bio potreban poseban zakon kojim se točno opisuje primjena i uvjeti za njezinu upotrebu. To osobito obuhvaća vrste kaznenih djela i, ako je primjenjivo, odgovarajući prag težine tih kaznenih djela kako bi se, među ostalim, učinkovito isključila lakša kaznena djela.[15]

3.1.3.2 Bit temeljnog prava na privatnost i zaštitu osobnih podataka utvrđenog u člancima 7. i 8. Povelje

45. Ograničenjima temeljnih prava koja su neminovna u svakoj situaciji i dalje se mora osigurati bit određenog prava koje treba poštovati. Bit se odnosi na samu osnovu relevantnog temeljnog prava[16]. Također se mora poštovati ljudsko dostojanstvo, čak i kada je pravo ograničeno[17].

46. Naznake mogućeg kršenja nepovredive osnove prava jesu sljedeće:

- odredba kojom se nameću ograničenja, neovisno o pojedinačnom ponašanju osobe ili iznimnim okolnostima[18]
- nije se moguće obratiti sudu ili je ostvarenje tog prava otežano[19]
- prije strogog ograničenja ne uzimaju se u obzir osobne okolnosti predmetnog pojedinca[20]

[13] ESLJP, Shimovolos protiv Rusije, t. 68.; Vukota-Bojić protiv Švicarske.
[14] ESLJP, Piechowicz protiv Poljske, t. 212.
[15] Vidjeti primjerice presude Suda Europske unije u predmetu C-817/19 Ligue des droits humains, t. 151.f, i u predmetu C-207/16 Ministerio Fiscal, t. 56.
[16] Sud EU-a C-279/09, RoC 2010 I-13849, t. 60.
[17] Objašnjenja koja se odnose na Povelju o temeljnim pravima, glava I., Obrazloženje članka 1., SL C 303, 14.12.2007., str. 17.–35.
[18] Sud EU-a, C-601/15, t. 52.
[19] Sud EU-a, C-400/10, RoC 2010 I-08965, t. 55.
[20] Sud EU-a, C-408/03, RoC 2006 I-02647, t. 68.

- u odnosu na prava iz članaka 7. i 8. Povelje osim opsežnog prikupljanja metapodataka o komunikaciji, stjecanje saznanja o sadržaju elektroničke komunikacije mogla bi se prekršiti bit tih prava[21]
- u odnosu na prava iz članaka 7., 8. i 11. Povelje zakonodavstvo kojim se propisuje da pružatelji pristupa javnim internetskim komunikacijskim uslugama i pružatelji usluga smještaja informacija na poslužitelju smiju općenito i neselektivno zadržavati, među ostalim, osobne podatke koji se odnose na te usluge[22]
- u odnosu na prava iz članka 8. Povelje nedostatak osnovnih načela zaštite podataka i sigurnosti podataka također bi mogao ugroziti osnovu samog prava[23].

3.1.3.3 Legitiman cilj

47. Kako je objašnjeno u točki 3.1.3., ograničenja temeljnih prava moraju zaista ispunjavati ciljeve od općeg interesa koje priznaje Europska unija ili potrebu za zaštitom prava i sloboda drugih osoba.

48. Unija priznaje ciljeve navedene u članku 3. Ugovora o Europskoj uniji i druge interese zaštićene posebnim odredbama Ugovorâ[24], među ostalim područje slobode, sigurnosti i pravde, sprečavanje i suzbijanje kriminala. U svojim odnosima sa svijetom Unija bi općenito trebala doprinijeti miru i sigurnosti te zaštiti ljudskih prava.

49. Potreba za zaštitom prava i sloboda drugih odnosi se na prava osoba zaštićenih pravom Europske unije ili njezinih država članica. Procjena se mora provesti s ciljem usklađivanja zahtjevâ u pogledu zaštite odgovarajućih prava i postizanja pravedne ravnoteže među njima[25].

3.1.3.4 Ispitivanje nužnosti i proporcionalnosti

50. U pogledu zadiranja u temeljna prava, opseg diskrecijske ovlasti nacionalnog zakonodavca i zakonodavca Unije može se pokazati ograničenim, što ovisi o nizu čimbenika, uključujući područje o kojem je riječ, narav predmetnog prava koje je zajamčeno Poveljom, narav i težinu zadiranja u prava, kao i njegovu svrhu[26]. Zakonodavne mjere moraju biti primjerene za postizanje legitimnih ciljeva predmetnog zakonodavstva. Osim toga, mjera ne smije prelaziti granice onoga što je prikladno i nužno za ostvarenje tih ciljeva[27]. Cilj u općem interesu, koliko god bio temeljan, ne može sâm po sebi opravdati ograničenje temeljnog prava[28].

51. U skladu s ustaljenom sudskom praksom Suda EU-a, odstupanja i ograničenja u zaštiti osobnih podataka moraju se primjenjivati samo u granicama onog što je strogo nužno[29]. To također podrazumijeva da ne postoje manje invazivna sredstva dostupna za postizanje svrhe. Moguće alternative kao što su, ovisno o svrsi, dodatno osoblje, učestalija policijska kontrola ili dodatna ulična

[21] Sud EU-a – 203/15 – Tele2 Sverige, t. 101 s upućivanjem na predmete C-293/12 i C-594/12, t. 39.
[22] Sud EU-a, C-512/18, La Quadrature du Net, t. 209. i sljedeće
[23] Sud EU-a – C-594/12, t. 40.
[24] Objašnjenja koja se odnose na Povelju o temeljnim pravima, glava I., Obrazloženje članka 52., SL C 303, 14.12.2007., str. 17.–35.
[25] Jarass GrCh, 3. Aufl. 2016., EU-Grundrechte-Charta Art. 52 Rn. 31.–32.
[26] Sud EU-a – C-594/12, t. 47., sa sljedećim izvorima: vidjeti, prema analogiji, u pogledu članka 8. Europske konvencije o ljudskim pravima, ESLJP, S. i Marper protiv Ujedinjene Kraljevine [VV], br. 30562/04 i 30566/04, t. 102., EKLJP 2008-V.
[27] Sud EU-a – C-594/12, t. 46., sa sljedećim izvorima: Predmet C-343/09 Afton Chemical EU:C:2010:419, t. 45.; Volker und Markus Schecke i Eifert EU:C:2010:662, t. 74.; predmeti C-581/10 i C-629/10 Nelson i drugi EU:C:2012:657, t. 71.; predmet C-283/11 Sky Österreich EU:C:2013:28, t. 50.; i predmet C-101/12 Schaible EU:C:2013:661, t. 29.
[28] Sud EU-a – C-594/12, t. 51.
[29] Sud EU-a – C-594/12, t. 52., sa sljedećim izvorima: Predmet C-473/12 IPI EU:C:2013:715, t. 39. i navedena sudska praksa.

rasvjeta moraju se pažljivo utvrditi i procijeniti. Zakonodavne mjere trebale bi razlikovati i biti usmjerene na osobe koje su njima obuhvaćene s obzirom na cilj, kao što je borba protiv teških kaznenih djela. Ako mjera općenito obuhvaća sve osobe bez takvog razlikovanja, ograničenja ili iznimke, njome se pojačava zadiranje u prava[30]. Zadiranje u prava također se pojačava ako obrada podataka obuhvaća znatan dio stanovništva[31].

52. Zaštita osobnih podataka koja proizlazi iz izričite obveze predviđene u članku 8. stavku 1. Povelje ima osobitu važnost za pravo na poštovanje privatnog života iz njezina članka 7.[32] Zakonodavstvom moraju biti predviđena jasna i precizna pravila kojima se uređuju doseg i primjena mjere o kojoj je riječ te moraju biti propisani minimalni uvjeti na način da osobe čiji su podatci zadržani raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih osobnih podataka od rizika zloporabe, kao i od svih nezakonitih pristupa i korištenja tih podataka[33]. Nužnost raspolaganja takvim jamstvima još je značajnija ako su osobni podatci podvrgnuti automatskoj obradi te postoji značajan rizik od nezakonitog pristupa tim podatcima[34]. Nadalje, interno ili vanjsko, npr. sudsko, odobrenje uvođenja tehnologije prepoznavanja lica također može doprinijeti kao postupovno jamstvo i može se pokazati potrebnim u određenim slučajevima teškog zadiranja u prava.[35]

53. Utvrđena pravila moraju se prilagoditi specifičnoj situaciji, npr. količini obrađenih podataka, prirodi podataka[36] i riziku od nezakonitog pristupa podatcima. To zahtijeva pravila koja bi za cilj osobito imala uređivanje na jasan i strog način zaštite i sigurnosti podataka o kojima je riječ kako bi se jamčio njihov puni integritet i povjerljivost[37].

54. U odnosu između voditelja obrade i izvršitelja obrade, izvršiteljima obrade ne bi trebalo dopustiti da pri utvrđivanju razine sigurnosti koju primjenjuju na osobne podatke uzimaju u obzir samo gospodarska razmatranja, što bi moglo ugroziti dovoljno visoku razinu zaštite[38].

55. Pravnim aktom moraju se utvrditi materijalni i postupovni uvjeti te objektivni kriteriji na temelju kojih se određuju ograničenja pristupa nadležnih tijela podatcima i njihova naknadna upotreba. Za potrebe suzbijanja, otkrivanja ili kaznenog progona, predmetna kaznena djela trebala bi se smatrati dovoljno teškima za opravdanje opsega i težine takvog zadiranja u temeljna prava utvrđena, primjerice, u člancima 7. i 8. Povelje[39].

56. Podatci se moraju obrađivati na način kojim se osiguravaju primjenjivost i učinak pravila EU-a o zaštiti podataka, posebno onih predviđenih člankom 8. Povelje, u kojem se navodi da usklađenost sa

[30] Sud EU-a – C-594/12, t. 57.
[31] Sud EU-a – C-594/12, t. 56.
[32] Sud EU-a – C-594/12, t. 53.
[33] Sud EU-a – C-594/12, t. 54., sa sljedećim izvorima: vidjeti, prema analogiji, u pogledu članka 8. Europske konvencije o ljudskim pravima, ESLJP, Liberty i drugi protiv Ujedinjene Kraljevine, 1. srpnja 2008., br. 58243/00, t. 62. i 63.; Rotaru protiv Rumunjske, t. 57. do 59., i S. i Marper protiv Ujedinjene Kraljevine, t. 99.
[34] Sud EU-a – C-594/12, t. 55., sa sljedećim izvorima: vidjeti, prema analogiji, u pogledu članka 8. Europske konvencije o ljudskim pravima, S. i Marper protiv Ujedinjene Kraljevine, t. 103., i M. K. protiv Francuske, 18. travnja 2013., br. 19522/09, t. 35.
[35] ESLJP, Szabó i Vissy protiv Mađarske, t. 73.–77.
[36] Vidjeti također pooštrene zahtjeve za tehničke i organizacijske mjere pri obradi posebnih kategorija podataka, članak 29. stavak 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.
[37] Sud EU-a – C-594/12, t. 66.
[38] Sud EU-a – C-594/12, t. 67.
[39] Sud EU-a – C-594/12, t. 60. i 61.

zahtjevima zaštite i sigurnosti podliježe nadzoru neovisnog tijela. U takvoj situaciji može biti relevantno zemljopisno mjesto na kojem se odvija obrada[40].

57. Kod različitih faza obrade osobnih podataka trebalo bi razlikovati kategorije podataka na temelju njihove moguće korisnosti za potrebe cilja koji se želi postići ili ovisno o predmetnim osobama[41]. Utvrđivanje uvjeta obrade, kao što je utvrđivanje trajanja zadržavanja, mora biti utemeljeno na objektivnim kriterijima kako bi se zajamčilo da je zadiranje u prava ograničeno na ono što je strogo nužno[42].

58. Na temelju svake situacije, procjenom nužnosti i proporcionalnosti moraju se utvrditi i razmotriti sve posljedice obuhvaćene područjem primjene drugih temeljnih prava, kao što su ljudsko dostojanstvo iz članka 1. Povelje, sloboda mišljenja, savjesti i vjeroispovijedi iz članka 10. Povelje, sloboda izražavanja iz članka 11. Povelje te sloboda okupljanja i udruživanja iz članka 12. Povelje.

59. Nadalje, u pogledu značajnosti utjecaja valja imati na umu da će sustavna obrada podataka bez znanja ispitanika vjerojatno stvoriti opću predodžbu o stalnom nadzoru[43], što može dovesti do odvraćajućih učinaka u pogledu nekih ili svih predmetnih temeljnih prava.

60. Kako bi se olakšala i operacionalizirala procjena nužnosti i proporcionalnosti u zakonodavnim mjerama povezanima s prepoznavanjem lica u području izvršavanja zakonodavstva, nacionalni zakonodavci i zakonodavci Unije mogu upotrijebiti dostupne praktične alate posebno osmišljene za tu aktivnost. Konkretno bi se mogao upotrijebiti skup alata za nužnost i proporcionalnost[44] koji osigurava EDPS.

3.1.3.5 Članak 52. stavak 3., članak 53. Povelje (razina zaštite, također u odnosu na razinu zaštite zajamčenu Konvencijom)

61. U skladu s člankom 52. stavkom 3. i člankom 53. Povelje, značenje i područje primjene iz Povelje koja odgovaraju pravima zajamčenima Konvencijom jednaki su onima iz navedene Konvencije. Iako se u Konvenciji posebno za članak 7. Povelje može pronaći istovjetna odredba, to nije slučaj s člankom 8. Povelje[45]. Članak 52. stavak 3. Povelje ne sprječava pravo Unije da pruži širu zaštitu. Budući da Konvencija ne predstavlja pravni instrument koji je formalno ugrađen u pravo EU-a, zakonodavstvo EU-a mora se provoditi u skladu s temeljnim pravima iz Povelje[46].

62. U skladu s člankom 8. Konvencije, država se ne smije miješati u ostvarivanje prava na poštovanje privatnog i obiteljskog života, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira ili gospodarske dobrobiti zemlje, te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala odnosno za zaštitu prava i sloboda drugih.

63. Konvencijom se također utvrđuju standardi u pogledu načina na koji se mogu provoditi ograničenja. Jedan od osnovnih zahtjeva osim vladavine prava jest predvidljivost. Kako bi se ispunio zahtjev u pogledu predvidljivosti, domaće pravo mora biti dovoljno jasno kako bi se pojedincima pružile odgovarajuće informacije o okolnostima i uvjetima pod kojima su nadležna tijela ovlaštena pribjeći

[40] Sud EU-a – C-594/12, t. 68.
[41] Sud EU-a – C-594/12, t. 63.
[42] Sud EU-a – C-594/12, t. 64.
[43] Sud EU-a – C-594/12, t. 37.
[44] Europski nadzornik za zaštitu podataka: Procjena nužnosti mjera kojima se ograničava temeljno pravo na zaštitu osobnih podataka: priručnik (11.4.2017.); Europski nadzornik za zaštitu podataka: Smjernice EDPS-a o procjeni proporcionalnosti mjera kojima se ograničavaju temeljna prava na privatnost i zaštitu osobnih podataka) (19.12.2019.).
[45] Sud EU-a – C-203/15 – Tele2 Sverige, t. 129.
[46] Sud EU-a – C-311/18, t. 99.

takvim ograničenjima[47]. Taj zahtjev potvrđuju Sud EU-a i zakonodavstvo EU-a o zaštiti podataka (usp. odjeljak 3.2.1.1.).

64. Dodatno određujući prava iz članka 8. Konvencije, također se moraju u potpunosti poštovati odredbe Konvencije o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka[48]. Međutim, treba uzeti u obzir da te odredbe predstavljaju samo minimalni standard s obzirom na prevladavajuće pravo Unije.

3.2 Konkretni pravni okvir – Direktiva o zaštiti podataka pri izvršavanju zakonodavstva

65. Određeni okvir za upotrebu tehnologiju prepoznavanja lica predviđen je Direktivom o zaštiti podataka pri izvršavanju zakonodavstva. Prije svega, u članku 3. stavku 13. Direktive o zaštiti podataka pri izvršavanju zakonodavstva definiran je pojam „biometrijski podatci"[49]. Pojedinosti su navedene u prethodnom odjeljku 2.1. Drugo, u članku 8. stavku 2. pojašnjava se da, kako bi svaka obrada bila zakonita, osim što mora biti nužna za svrhe navedene u članku 1. stavku 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, ta obrada također mora biti uređena nacionalnim pravom kojim se utvrđuju barem ciljevi obrade, osobni podatci za obradu i svrhe obrade. Daljnje odredbe od posebne važnosti u pogledu biometrijskih podataka jesu članci 10. i 11. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. Članak 10. mora se čitati u vezi s člankom 8. Direktive o zaštiti podataka pri izvršavanju zakonodavstva[50]. Uvijek treba poštovati načela za obradu osobnih podataka kako su utvrđena u članku 4. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, a svaka procjena moguće biometrijske obrade putem tehnologije prepoznavanja lica trebala bi se voditi tim načelima.

3.2.1 Obrada posebnih kategorija podataka za potrebe izvršavanja zakonodavstva

66. U skladu s člankom 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, obrada posebnih kategorija podataka, kao što su biometrijski podatci, dopuštena je samo ako je to nužno, uz poštovanje odgovarajućih postupovnih jamstava u pogledu prava i sloboda ispitanika. Osim toga, ako je to dopušteno pravom Unije ili pravom države članice, takva je obrada dopuštena samo u svrhu zaštite vitalnih interesa ispitanika ili druge fizičke osobe odnosno ako se takva obrada odnosi na podatke koje je osoba čiji se podatci obrađuju očito objavila. Tom se općom odredbom naglašava osjetljivost obrade posebnih kategorija podataka.

3.2.1.1 Dopušteno pravom Unije ili države članice

67. U pogledu potrebne vrste zakonodavne mjere, u uvodnoj izjavi 33. Direktive o zaštiti podataka pri izvršavanju zakonodavstva navedeno je sljedeće: „Ako se ovom Direktivom upućuje na pravo države članice, pravnu osnovu ili zakonodavnu mjeru, to ne znači nužno da parlament mora donijeti

[47] Europski sud za ljudska prava, presuda, predmet Copland protiv Ujedinjene Kraljevine, 3. travnja 2007., br. 62617/00, t. 46.
[48] ETS br. 108.
[49] Članak 3. stavak 13. Direktive o zaštiti podataka pri izvršavanju zakonodavstva: „biometrijski podaci" znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.
[50] WP258, Mišljenje o nekim ključnim pitanjima iz Direktive o izvršavanju zakonodavstva (EU 2016/680), str. 7.

zakonodavni akt, ne dovodeći u pitanje zahtjeve u skladu s ustavnim poretkom dotične države članice".[51]

68. U skladu s člankom 52. stavkom 1. Povelje, svako ograničenje pri ostvarivanju prava i sloboda priznatih Poveljom mora biti „predviđeno zakonom". U tome se prepoznaje izraz „u skladu sa zakonom" iz članka 8. stavka 2. Konvencije, koji se odnosi ne samo na poštovanje nacionalnog prava, nego i na kvalitetu tog prava, ne dovodeći u pitanje prirodu akta, pri čemu ono mora biti usklađeno s vladavinom prava.

69. U uvodnoj izjavi 33. Direktive o zaštiti podataka pri izvršavanju zakonodavstva navodi se sljedeće: „Međutim, takvo pravo države članice, pravna osnova ili zakonodavna mjera trebala bi biti jasna i precizna, a njezina primjena trebala bi biti predvidljiva osobama na koje se primjenjuje sukladno sudskoj praksi Suda i Europskog suda za ljudska prava. U pravu države članice kojim se uređuje obrada osobnih podataka unutar područja primjene ove Direktive trebali bi se navesti barem ciljevi, osobni podaci koji se obrađuju, svrhe obrade i postupci za očuvanje cjelovitosti i povjerljivosti osobnih podataka te postupci za njihovo uništenje."

70. Nacionalno pravo mora biti dovoljno jasno kako bi se ispitanicima pružile odgovarajuće informacije o okolnostima i uvjetima pod kojima voditelji obrade mogu pribjeći takvim mjerama, što uključuje moguće preduvjete za obradu, kao što su posebne vrste dokaza te nužnost sudskog ili internog odobrenja. Odgovarajuće pravo može biti tehnološki neutralno ako su u dovoljnoj mjeri uzeti u obzir posebni rizici i značajke obrade osobnih podataka u sustavima tehnologije prepoznavanja lica. U skladu s Direktivom o zaštiti podataka pri izvršavanju zakonodavstva, sudskom praksom Suda Europske unije i Europskog suda za ljudska prava (ESLJP), od ključne je važnosti da su zakonodavne mjere, čiji je cilj pružiti pravnu osnovu za mjeru za prepoznavanje lica, predvidljive ispitanicima.

71. Na zakonodavnu mjeru ne može se pozivati kao na zakon kojim se dopušta obrada biometrijskih podataka primjenom tehnologije prepoznavanja lica za potrebe izvršavanja zakonodavstva ako je riječ samo o prenošenju opće klauzule iz članka 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

72. Osim biometrijskih podataka, člankom 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva također se uređuje obrada drugih posebnih kategorija podataka, kao što su seksualna orijentacija, politička mišljenja i vjera, čime je obuhvaćen širok raspon obrade. Osim toga, takvoj bi odredbi nedostajali posebni zahtjevi koji bi ukazivali na okolnosti i uvjete u kojima bi tijela za izvršavanje zakonodavstva bila ovlaštena upotrebljavati tehnologiju prepoznavanja lica. Zbog upućivanja na druge vrste podataka i izričite potrebe za posebnim postupovnim jamstvima bez dodatnih specifikacija, nije se moguće pozivati na nacionalnu odredbu kojom se u nacionalno pravo prenosi članak 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva (sa sličnim općenitim i apstraktnim tekstom) kao na pravnu osnovu za obradu biometrijskih podataka koja uključuje prepoznavanje lica jer ne bi bila dovoljno precizna i predvidljiva. U skladu s člankom 28. stavkom 2. ili člankom 46. stavkom 1. točkom (c) Direktive o zaštiti podataka pri izvršavanju zakonodavstva, prije nego što nacionalni zakonodavac stvori novu pravnu osnovu za svaki oblik obrade biometrijskih podataka s pomoću prepoznavanja lica, treba provesti savjetovanje s nacionalnim nadzornim tijelom za zaštitu podataka.

[51] Vrsta razmatranih zakonodavnih mjera mora biti u skladu s pravom EU-a ili nacionalnim pravom. Ovisno o stupnju u kojem ograničenje zadire u prava, određena zakonodavna mjera mogla bi se propisati na nacionalnoj razini, uzimajući u obzir razinu norme.

3.2.1.2 Strogo nužna obrada

73. Obrada se može smatrati „strogo nužnom" samo ako su zadiranje u zaštitu osobnih podataka i njezina ograničenja ograničeni na ono što je apsolutno nužno[52]. Dodavanje izraza „strogo" znači da zakonodavac propisuje obradu posebnih kategorija podataka samo u uvjetima koji su stroži od uvjeta nužnosti (vidjeti prethodnu točku 3.1.3.4.). Taj se zahtjev treba tumačiti kao neophodan. Njime se margina prosudbe kojom raspolaže tijelo za izvršavanje zakonodavstva u okviru ispitivanja nužnosti svodi na apsolutni minimum. U skladu s ustaljenom sudskom praksom Suda EU-a, uvjet „stroge nužnosti" također je usko povezan sa zahtjevom objektivnih kriterija kako bi se definirale okolnosti i uvjeti u kojima se obrada može provoditi, čime se isključuje svaka obrada opće ili sustavne naravi[53].

3.2.1.3 Očito objavljeni podatci

74. Kada se procjenjuje odnosi li se obrada na podatke koje je očito objavio ispitanik, treba podsjetiti da se fotografija kao takva sustavno ne smatra biometrijskim podatkom[54]. Stoga činjenica da je fotografiju očito objavio ispitanik ne znači da se smatra da su očito objavljeni povezani biometrijski podatci koji se mogu preuzeti s fotografije posebnim tehničkim sredstvima.

75. U pogledu osobnih podataka općenito, kako bi se smatralo da je ispitanik očito objavio biometrijske podatke, ispitanik mora namjerno staviti biometrijski predložak (a ne samo prikaz lica) na raspolaganje javnosti putem otvorenog izvora. Ako treća strana otkrije biometrijske podatke, ne može se smatrati da je ispitanik očito objavio podatke.

76. Osim toga, nije dovoljno tumačiti ponašanje ispitanika kako bi se smatralo da su biometrijski podatci očito objavljeni. Primjerice, u pogledu društvenih mreža ili internetskih platformi, EDPB smatra da činjenica da ispitanik nije aktivirao ili postavio posebne značajke privatnosti nije dovoljna za stav da je očito kako je taj ispitanik objavio svoje osobne podatke i da se ti podatci (npr. fotografije) smiju obrađivati u svrhu izrade biometrijskih predložaka i upotrebljavati u svrhu identifikacije bez privole ispitanika. Općenito zadane postavke usluge, kao što je stavljanje predložaka na raspolaganje javnosti ili izostanak mogućnosti izbora, primjerice kada se predlošci objavljuju bez mogućnosti da korisnik promijeni tu postavku, ni na koji način ne bi trebalo tumačiti kao podatke koji su očito objavljeni.

3.2.2 Automatizirano pojedinačno donošenje odluka, uključujući izradu profila

77. Člankom 11. stavkom 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva državama članicama propisuje se obveza da općenito zabrane odluke utemeljene samo na automatiziranoj obradi, među ostalim i na izradi profila, koja proizvodi negativne pravne učinke za ispitanika ili na njega znatno utječe. Kao izuzeće od te opće zabrane, takva obrada moguća je samo ako je dopuštena pravom Unije ili pravom države članice koje se primjenjuje na voditelja obrade i kojim se osiguravaju odgovarajuća postupovna jamstva za prava i slobode ispitanika, barem pravo na intervenciju voditelja obrade (ljudska intervencija). Smije se upotrebljavati samo ograničeno. Taj se prag primjenjuje na uobičajene (odnosno, ne posebne) kategorije osobnih podataka. Za izuzeće na temelju članka 11. stavka 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva primjenjuje se još viši prag i ograničenija upotreba. Njime se ponovno naglašava da se odluke iz prvog stavka ne smiju temeljiti na posebnim kategorijama podataka, tj. posebno biometrijskim podatcima u svrhu jedinstvene identifikacije fizičke

[52] Ustaljena sudska praksa u području temeljnog prava na poštovanje privatnog života, vidjeti predmete Suda EU-a C-73/07, t. 56. (Satakunnan Markkinapörssi i Satamedia); C-92/09 i C-93/09, t. 77. (Schecke i Eifert); C-594/12, t. 52. (Digitalna prava); C-362/14, t. 92. (Schrems).

[53] Sud EU-a, predmet C-623/17, t. 78.

[54] Usp. uvodnu izjavu 51. OUZP-a: „Obradu fotografija ne bi trebalo sustavno smatrati obradom posebnih kategorija osobnih podataka jer su one biti obuhvaćene samo definicijom biometrijskih podataka pri obradi posebnim tehničkim sredstvima kojima se omogućuje jedinstvena identifikacija ili autentifikacija pojedinca."

osobe. Izuzeće se smije predvidjeti samo ako su uspostavljene odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa predmetnog pojedinca. To se izuzeće mora tumačiti kao dodatak i na temelju načela iz članka 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

78. Ovisno o sustavu tehnologije prepoznavanja lica, čak i ljudska intervencija kojom se ocjenjuju rezultati tehnologije prepoznavanja lica ne mora nužno sama po sebi predstavljati dovoljno jamstvo u pogledu poštovanja pravâ pojedinaca, a posebno prava na zaštitu osobnih podataka, uzimajući u obzir moguću pristranost i pogrešku koji mogu proizaći iz same obrade. Nadalje, ljudska intervencija može se smatrati postupovnim jamstvom samo ako osoba koja intervenira može kritički osporiti rezultate tehnologije prepoznavanja lica tijekom ljudske intervencije. Ključno je osobi omogućiti razumijevanje sustava tehnologije prepoznavanja lica i njegovih ograničenja te pravilno tumačenje njegovih rezultata. Također je potrebno uspostaviti mjesto rada i organizaciju kojima se suzbijaju učinci pristranosti automatizacije te se izbjegava poticanje nekritičkog prihvaćanja rezultata, npr. zbog vremenskog pritiska, opterećujućih postupaka, mogućih štetnih učinaka na karijeru itd.

79. U skladu s člankom 11. stavkom 3.o zaštiti podataka pri izvršavanju zakonodavstva zabranjuje se izrada profila koja dovodi do diskriminacije pojedinaca na temelju posebnih kategorija osobnih podataka, kao što su biometrijski podatci, u skladu s pravom Unije. U skladu s člankom 3. stavkom 4. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, „izrada profila" predstavlja svaki oblik automatizirane obrade osobnih podataka koja podrazumijeva uporabu osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca. Kada se razmatra jesu li predviđene odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa dotičnog pojedinca, valja imati na umu da upotreba tehnologije prepoznavanja lica može dovesti do izrade profila, ovisno o načinu i svrsi primjene tehnologije prepoznavanja lica. U svakom slučaju, u skladu s pravom Unije i člankom 11. stavkom 3. Direktive o zaštiti podataka pri izvršavanju zakonodavstva zabranjuje se izrada profila koja dovodi do diskriminacije pojedinaca na temelju posebnih kategorija osobnih podataka.

3.2.3 Kategorije ispitanikâ

80. Članak 6. Direktive o zaštiti podataka pri izvršavanju zakonodavstva odnosi se na potrebu razlikovanja različitih kategorija ispitanika. Ta se razlika mora napraviti kad je to primjenjivo i u najvećoj mogućoj mjeri. Mora pokazati učinak u načinu na koji se podatci obrađuju. Iz primjera navedenih u članku 6. Direktive o zaštiti podataka pri izvršavanju zakonodavstva može se zaključiti da obrada osobnih podataka u pravilu također mora ispunjavati kriterije nužnosti i proporcionalnosti s obzirom na kategoriju ispitanika[55]. Nadalje, može se zaključiti da u pogledu ispitanika za koje ne postoje dokazi koji bi upućivali na povezanost s njihovim ponašanjem, čak i neizravnu ili udaljenu, s legitimnim ciljem na temelju Direktive o zaštiti podataka pri izvršavanju zakonodavstva, najvjerojatnije ne postoji opravdanje za zadiranje u prava[56]. Ako razlika u skladu s člankom 6. Direktive o zaštiti podataka pri izvršavanju zakonodavstva nije primjenjiva ili moguća, iznimka od pravila iz članka 6. Direktive mora se strogo uzeti u obzir pri ocjenjivanju nužnosti i proporcionalnosti zadiranja u prava. Razlika između različitih kategorija ispitanika mogla bi biti osnovni uvjet u pogledu obrade osobnih podataka koja uključuje prepoznavanje lica, također uzimajući u obzir moguće lažno pozitivne ili lažno negativne rezultate, koji mogu imati znatne učinke na ispitanike, kao i tijekom istrage.

81. Kao što je već navedeno, pri provedbi prava Unije moraju se poštovati odredbe Povelje Europske unije o temeljnim pravima, usp. članak 52. Povelje. Stoga okvir i kriterije predviđene Direktivom o zaštiti

[55] Usp. također Sud EU-a – C-594/12, t. 56.–59.
[56] Usp. također Sud EU-a – C-594/12, t. 58.

podataka pri izvršavanju zakonodavstva treba tumačiti u skladu s Poveljom. Pravni akti EU-a i njegovih država članica ne smiju biti blaži te mjere i njima mora biti osiguran puni učinak Povelje.

3.2.4 Prava ispitanika

82. EDPB već je pružio smjernice o pravima ispitanikâ na temelju OUZP-a u različitim aspektima[57]. Direktivom o zaštiti podataka pri izvršavanju zakonodavstva predviđena su slična prava ispitanika, a opće smjernice o tome iznesene su u mišljenju Radne skupine iz članka 29., koje je prihvatio EDPB[58]. U određenim okolnostima Direktivom o zaštiti podataka pri izvršavanju zakonodavstva dopuštena su određena ograničenja tih prava. Parametri za takva ograničenja dodatno su razrađeni u odjeljku 3.2.4.6. „Legitimna ograničenja pravâ ispitanika".

83. Iako se sva prava ispitanika navedena u poglavlju III. Direktive o zaštiti podataka pri izvršavanju zakonodavstva također primjenjuju na obradu osobnih podataka primjenom tehnologije prepoznavanja lica, u sljedećem poglavlju naglasak će biti na nekim pravima i aspektima koji bi mogli biti od posebnog interesa za dobivanje smjernica. Nadalje, ovo poglavlje i njegova analiza temelje se na pretpostavci da je predmetna obrada s pomoću tehnologije prepoznavanja lica u skladu s pravnim zahtjevima opisanim u prethodnom poglavlju.

84. S obzirom na prirodu obrade osobnih podataka s pomoću tehnologije prepoznavanja lica (obrada posebnih kategorija osobnih podataka često bez ikakve očite interakcije s ispitanikom), voditelj obrade mora pažljivo razmotriti pitanje poštovanja odredbi Direktive o zaštiti podataka pri izvršavanju zakonodavstva prije pokretanja bilo kakve obrade tehnologijom prepoznavanja lica, odnosno može li uopće ispuniti te odredbe. To se postiže osobito pažljivom analizom sljedećih pitanja:

- tko su ispitanici (često se radi o više ispitanika koji su glavni cilj za potrebe obrade)
- kako su ispitanici upoznati s obradom uz pomoć tehnologije prepoznavanja lica (vidjeti odjeljak 3.2.4.1.)
- kako ispitanici mogu ostvariti svoja prava (pri čemu može biti osobito zahtjevno poštovati prava na informacije i pristup, kao i prava na ispravak ili ograničenje, ako se tehnologija prepoznavanja lica upotrebljava za bilo što osim za provjeru usporedbom dvaju uzoraka u izravnom kontaktu s ispitanikom).

3.2.4.1 Informiranje ispitanikâ o pravima i informacijama u sažetom, razumljivom i lako dostupnom obliku

85. Tehnologija prepoznavanja lica donosi izazove u pogledu osiguravanja toga da su ispitanici svjesni svojih biometrijskih podataka koji se obrađuju. Posebno je zahtjevno ako tijelo za izvršavanje zakonodavstva provodi analizu putem videomaterijala dobivenog tehnologijom prepoznavanja lica koji potječe od treće strane ili ga treća strana nudi jer tijelo za izvršavanje zakonodavstva ima malu, odnosno u većini slučajeva nikakvu, mogućnost obavijestiti ispitanika u trenutku prikupljanja (npr. putem znaka na licu mjesta). Svi videomaterijali koji nisu relevantni za istragu (ili svrhu obrade) uvijek bi se trebali ukloniti ili anonimizirati (npr. zamagljivanjem bez mogućnosti retroaktivnog oporavka podataka) prije uvođenja bilo kakve obrade biometrijskih podataka kako bi se izbjegao rizik od neispunjavanja načela smanjenja količine podataka iz članka 4. stavka 1. točke (e) Direktive o zaštiti podataka pri izvršavanju zakonodavstva i obveza informiranja iz članka 13. stavka 2. te Direktive. Voditelj obrade dužan je ocijeniti koje bi informacije bile važne ispitaniku u ostvarivanju njegovih prava

[57] Vidjeti, primjerice, smjernice EDPB-a 1/2022 o pravima ispitanika – Pravo na pristup i smjernice EDPB-a 3/2019 o obradi osobnih podataka putem videouređaja.
[58] WP258, Mišljenje o nekim ključnim pitanjima iz Direktive o zaštiti podataka pri izvršavanju zakonodavstva (EU 2016/680).

i osigurati pružanje potrebnih informacija. Učinkovito ostvarivanje prava ispitanika ovisi o tome ispunjava li voditelj obrade svoje obveze pružanja informacija.

86. Člankom 13. stavkom 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva propisuje se koje minimalne informacije treba pružiti ispitaniku. Te se informacije mogu pružiti putem mrežnog mjesta voditelja obrade, u tiskanom obliku (npr. letak dostupan na zahtjev) ili putem drugih izvora lako dostupnih za ispitanika. Voditelj obrade u svakom slučaju mora osigurati da se informacije učinkovito pružaju barem za sljedeće elemente:

- identitet i podatke za kontakt voditelja obrade, uključujući službenika za zaštitu podataka
- svrhu obrade i činjenicu da se obrada provodi primjenom tehnologije prepoznavanja lica
- pravo na podnošenje pritužbe nadzornom tijelu i podatke za kontakt tog tijela
- pravo na traženje pristupa osobnim podatcima, na njihov ispravak ili brisanje te ograničavanje obrade osobnih podataka.

87. Osim toga, u posebnim slučajevima definiranim u nacionalnom pravu, koji bi trebali biti u skladu s člankom 13. stavkom 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva[59], kao što je, primjerice, obrada primjenom tehnologije prepoznavanja lica, sljedeće informacije moraju se izravno pružiti ispitaniku:

- pravna osnova za obradu podataka
- informacije o tome gdje su osobni podatci prikupljeni bez znanja ispitanika
- razdoblje u kojem će se osobni podatci pohranjivati ili, ako to nije moguće, kriteriji korišteni za utvrđivanje tog razdoblja
- ako je primjenjivo, kategorije primatelja osobnih podataka (uključujući treće zemlje ili međunarodne organizacije).

88. Iako se članak 13. stavak 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva odnosi na opće informacije koje se stavljaju na raspolaganje javnosti, članak 13. stavak 2. Direktive odnosi se na dodatne informacije koje se moraju pružiti određenom ispitaniku u posebnim slučajevima, na primjer ako se podatci prikupljaju izravno od ispitanika ili neizravno bez znanja ispitanika[60]. U članku 13. stavku 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva ne postoji jasna definicija pojma „određeni slučajevi". Međutim, odnosi se na situacije u kojima ispitanici moraju biti obaviješteni o obradi koja se konkretno odnosi na njih i dobiti odgovarajuće informacije kako bi učinkovito ostvarili svoja prava. Kada se ocjenjuje postoji li „određeni slučaj", EDPB smatra da je potrebno uzeti u obzir nekoliko čimbenika, među ostalim pitanje prikupljaju li se osobni podatci bez znanja ispitanika, jer bi to bio jedini način da se ispitanicima omogući učinkovito ostvarivanje njihovih prava. Drugi primjeri „određenih slučajeva" mogli bi biti slučajevi u kojima se osobni podatci dalje obrađuju u okviru postupka međunarodne kaznene suradnje ili u situaciji kada se osobni podatci obrađuju u okviru tajnih operacija, kako je navedeno u nacionalnom pravu. Nadalje, iz uvodne izjave 38. Direktive o zaštiti podataka pri izvršavanju zakonodavstva proizlazi da, ako se odluke donose isključivo na temelju tehnologije prepoznavanja lica, ispitanici moraju biti obaviješteni o značajkama automatiziranog

[59] Primjerice, članak 56. stavak 1. njemačkog Saveznog zakona o zaštiti podataka, u kojem se, među ostalim, navodi koje informacije treba pružiti ispitanicima u tajnim postupcima

[60] WP258, Mišljenje o nekim ključnim pitanjima iz Direktive o izvršavanju zakonodavstva (EU 2016/680), str. 17.–18.

donošenja odluka. To bi također podrazumijevalo da je to određeni slučaj u kojem ispitaniku treba pružiti dodatne informacije u skladu s člankom 13. stavkom 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva[61].

89. Konačno, treba napomenuti da u skladu s člankom 13. stavkom 3. Direktive o zaštiti podataka pri izvršavanju zakonodavstva države članice mogu donijeti zakonodavne mjere kojima se ograničava obveza pružanja informacija u određenim slučajevima za određene ciljeve. To se primjenjuje u mjeri u kojoj i ako takva mjera predstavlja nužnu i razmjernu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa ispitanika.

3.2.4.2 Pravo na pristup

90. Općenito, ispitanik ima pravo dobiti pozitivnu ili negativnu potvrdu o svakoj obradi svojih osobnih podataka te, ako je odgovor pozitivan, dobiti pristup osobnim podatcima kao takvima, kao i dodatnim informacijama, kako je navedeno u članku 14. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. U pogledu tehnologije prepoznavanja lica, kada se biometrijski podatci pohranjuju i povezuju s identitetom s pomoću alfanumeričkih podataka, time bi se nadležnom tijelu trebalo omogućiti da potvrdi zahtjev za pristup na temelju pretraživanja tih alfanumeričkih podataka bez pokretanja daljnje obrade biometrijskih podataka drugih osoba (pretraživanjem baze podataka s pomoću tehnologije prepoznavanja lica). Mora se poštovati načelo smanjenja količine podataka i ne smije se pohranjivati više podataka nego što je to potrebno s obzirom na svrhu obrade.

3.2.4.3 Pravo na ispravak osobnih podataka

91. Budući da tehnologija prepoznavanja lica ne jamči apsolutnu točnost, od posebne je važnosti da voditelji obrade budu oprezni u pogledu zahtjevâ za ispravak osobnih podataka. To može biti slučaj i kada je ispitanik na temelju tehnologije prepoznavanja lica uvršten u netočnu kategoriju, npr. ako je pogrešno uvršten u kategoriju osumnjičenika na temelju početnog postupanja na osnovu videozapisa. Rizici za ispitanike osobito su ozbiljni ako su takvi netočni podatci pohranjeni u policijskoj bazi podataka i/ili ako se dijele s drugim subjektima. Voditelj obrade u skladu s tim mora ispraviti pohranjene podatke i sustave tehnologije prepoznavanja lica. U tom smislu vidjeti uvodnu izjavu 47. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

3.2.4.4 Pravo na brisanje

92. Ako se ne upotrebljava za provjeru/autentifikaciju usporedbom dvaju uzoraka, tehnologija prepoznavanja lica u većini će slučajeva podrazumijevati obradu velikog broja biometrijskih podataka ispitanikâ. Stoga je važno da voditelj obrade unaprijed razmotri ograničenja njezine svrhe i nužnosti kako bi se zahtjev za brisanje u skladu s člankom 16. Direktive o zaštiti podataka pri izvršavanju zakonodavstva mogao obraditi bez nepotrebnog odlaganja (s obzirom na činjenicu da voditelj obrade među ostalim treba izbrisati osobne podatke koji se obrađuju izvan okvira onoga što je dopušteno primjenjivim zakonodavstvom u skladu s člancima 4., 8. i 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva).

3.2.4.5 Pravo na ograničenje

93. Ako ispitanik osporava točnost podataka, a točnost podataka nije moguće utvrditi (ili ako se osobni podatci moraju zadržati za potrebe budućih dokaza), voditelj obrade dužan je ograničiti osobne podatke tog ispitanika u skladu s člankom 16. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. To postaje osobito važno kada je riječ o tehnologiji prepoznavanja lica (na temelju

[61] Valja imati na umu razliku između „stavljanja na raspolaganje ispitaniku" iz članka 13. stavka 1. Direktive o zaštiti podataka pri izvršavanju zakonodavstva i „davanja ispitaniku" iz članka 13. stavka 2. te Direktive. U članku 13. stavku 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva navedeno je da voditelj obrade mora osigurati da će informacije doći do ispitanika ako informacije objavljene na mrežnom mjestu nisu dovoljne.

jednog ili više algoritama), što znači da se nikad ne prikazuje konačan rezultat u situacijama u kojima se prikupljaju velike količine podataka te može doći do odstupanja u pogledu točnosti i kvalitete identifikacije. Rizik od lažno pozitivnih rezultata povećava se u slučaju videomaterijala loše kvalitete (npr. videomaterijal s mjesta zločina). Nadalje, ako se prikazi lica na popisu za praćenje redovito ne ažuriraju, to će također povećati rizik od lažno pozitivnih ili lažno negativnih rezultata. U posebnim slučajevima, ako se podatci ne mogu izbrisati zbog činjenice da postoje opravdani razlozi za sumnju da bi brisanje moglo utjecati na legitimne interese ispitanika, podatke bi umjesto toga trebalo ograničiti i obrađivati samo u svrhu zbog koje nisu bili izbrisani (vidjeti uvodnu izjavu 47. Direktive o zaštiti podataka pri izvršavanju zakonodavstva).

3.2.4.6 Legitimna ograničenja pravâ ispitanika

94. U pogledu obveza voditelja obrade da pruži informacije i o pravu ispitanikâ na pristup, ograničenja su dopuštena samo ako su utvrđena zakonom, što mora predstavljati nužnu i razmjernu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa predmetnog pojedinca (vidjeti članak 13. stavak 3., članak 13. stavak 4., članak 15. i članak 16. stavak 4. Direktive o zaštiti podataka pri izvršavanju zakonodavstva). Ako se tehnologija prepoznavanja lica upotrebljava za potrebe izvršavanja zakonodavstva, može se očekivati da će se koristiti u okolnostima u kojima bi bilo štetno obavijestiti ispitanika ili omogućiti pristup podatcima u odnosu na svrhu koja se nastoji postići. To bi se, primjerice, primjenjivalo na policijsku istragu kaznenog djela ili u svrhu zaštite nacionalne ili javne sigurnosti.

95. Pravo na pristup ne podrazumijeva automatski pristup svim informacijama, primjerice u kaznenom predmetu u kojem se pojavljuju osobni podatci. Kaznena istraga predstavlja dobar primjer situacije u kojoj se mogu dopustiti ograničenja prava.

3.2.4.7 Ostvarivanje pravâ putem nadzornog tijela

96. U slučajevima kada postoje opravdana ograničenja u pogledu ostvarivanja pravâ u skladu s poglavljem III. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, ispitanik može zatražiti od tijela za zaštitu podataka da ostvari njegova prava u njegovo ime provjerom zakonitosti obrade koju provodi voditelj obrade. Voditelj obrade dužan je obavijestiti ispitanika o mogućnosti ostvarivanja njegovih prava na takav način (vidjeti članak 17. i članak 46. stavak 1. točku (g) Direktive o zaštiti podataka pri izvršavanju zakonodavstva). Kad je riječ o tehnologiji prepoznavanja lica, to znači da voditelj obrade mora osigurati postojanje odgovarajućih mjera kako bi se takav zahtjev mogao obraditi, npr. omogućivanje pretraživanja materijala, pod uvjetom da ispitanik pruži dovoljno informacija za pronalaženje njegovih osobnih podataka.

3.2.5 Ostali pravni zahtjevi i postupovna jamstva

3.2.5.1 Članak 27. Procjena učinka na zaštitu podataka

97. Procjena učinka na zaštitu podataka prije upotrebe tehnologije prepoznavanja lica obvezni je zahtjev jer je vjerojatno da će vrsta obrade, osobitom putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe te obrade, predstavljati visoki rizik za prava i slobode pojedinaca. S obzirom na to da upotreba tehnologije prepoznavanja lica podrazumijeva sustavnu automatsku obradu posebnih kategorija podataka, može se pretpostaviti da bi u takvim slučajevima voditelj obrade u pravilu morao provesti procjenu učinka na zaštitu podataka. Procjena učinka na zaštitu podataka trebala bi sadržavati barem opći opis predviđenih postupaka obrade, procjenu nužnosti i proporcionalnosti postupaka obrade u odnosu na svrhe, procjenu rizika za prava i slobode ispitanikâ, mjere predviđene za otklanjanje tih rizika, postupovna jamstva, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje usklađenosti. EDPB preporučuje objavljivanje rezultata takvih procjena

ili barem glavnih nalaza i zaključaka procjene učinka na zaštitu podataka kao mjeru za jačanje povjerenja i transparentnosti[62].

3.2.5.2 Članak 28. Prethodno savjetovanje s nadzornim tijelom

98. U skladu s člankom 28. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, voditelj obrade ili izvršitelj obrade prije obrade mora se savjetovati s nadzornim tijelom ako: (a) procjena učinka na zaštitu podataka upućuje na to da bi obrada mogla rezultirati visokim rizikom ako voditelj obrade ne poduzme mjere kako bi umanjio rizik ili (b) vrsta obrade, posebno ako se upotrebljavaju nove tehnologije, mehanizmi ili postupci, predstavlja visok rizik za prava i slobode ispitanikâ. Kako je već objašnjeno u odjeljku 2.3. ovih Smjernica, EDPB smatra da većina slučajeva uvođenja i upotrebe tehnologije prepoznavanja lica sama po sebi predstavlja visoki rizik za prava i slobode ispitanikâ. Stoga bi se, osim provedbe procjene učinka na zaštitu podataka, nadležno tijelo koje uvodi tehnologiju prepoznavanja lica trebalo savjetovati s nadležnim nadzornim tijelom prije uvođenja takvog sustava.

3.2.5.3 Članak 29. Sigurnost obrade

99. Jedinstvena priroda biometrijskih podataka onemogućuje ispitaniku da ih promijeni ako su ti podatci ugroženi, primjerice zbog njihove zlouporabe. Stoga bi nadležno tijelo koje provodi i/ili upotrebljava tehnologiju prepoznavanja lica trebalo pridati posebnu pozornost sigurnosti obrade u skladu s člankom 29. Direktive o zaštiti podataka pri izvršavanju zakonodavstva. Konkretno bi tijelo za izvršavanje zakonodavstva trebalo osigurati usklađenost sustava s relevantnim normama i provoditi mjere za zaštitu biometrijskih predložaka[63]. Ta je obveza još relevantnija ako tijelo za izvršavanje zakonodavstva upotrebljava pružatelja usluga (izvršitelja obrade podataka) treće strane.

3.2.5.4 Članak 20. Tehnička i integrirana zaštita podataka

100. U skladu s člankom 20. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, svrha tehničke i integrirane zaštite podataka jest osiguravanje da su načela i postupovna jamstva u pogledu zaštite podataka, kao što su smanjenje količine podataka i ograničenje pohrane, ugrađeni u tehnologiju putem odgovarajućih tehničkih i organizacijskih mjera, kao što je pseudonimizacija, čak i prije početka obrade osobnih podataka te da će se primjenjivati tijekom njezina životnog ciklusa. S obzirom na inherentno visoki rizik za prava i slobode pojedinaca, odabir takvih mjera ne bi trebao ovisiti samo o gospodarskim razmatranjima[64], nego bi cilj trebao biti provedba najnovijih dostignuća u tehnologijama zaštite podataka. Osim toga, čak i ako tijelo za izvršavanje zakonodavstva namjerava primjenjivati i upotrebljavati tehnologiju prepoznavanja lica vanjskih pružatelja usluga, mora osigurati, primjerice, putem postupka nabave, da se primjenjuje samo tehnologija prepoznavanja lica koja se temelji na načelima tehničke i integrirane zaštite podataka[65]. To također podrazumijeva da transparentnost u pogledu funkcioniranja tehnologije prepoznavanja lica nije ograničena zahtjevima o poslovnim tajnama ili pravima intelektualnog vlasništva.

3.2.5.5 Članak 25. Zapisivanje

101. Direktivom o zaštiti podataka pri izvršavanju zakonodavstva propisuju se različite metode kojima voditelj ili izvršitelj obrade mogu dokazati zakonitost obrade te za osiguravanje cjelovitosti i sigurnosti podataka. U tom pogledu zapisi sustava predstavljaju vrlo koristan alat i važno postupovno jamstvo za

---

[62] Za više informacija vidjeti dokument WP248 rev. 01 „Smjernice za procjenu učinka na zaštitu podataka i utvrđivanje je li ‚vjerojatno da će obrada predstavljati visoki rizik'".

[63] Primjerice, vidjeti sljedeće: ISO/IEC 24745 Informatička sigurnost, kibersigurnost i zaštita privatnosti – Zaštita biometrijskih informacija.

[64] Vidjeti uvodnu izjavu 53. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

[65] Za više informacija vidjeti Smjernice EDPB-a o tehničkoj i integriranoj zaštiti podataka, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

provjeru zakonitosti obrade, u internom smislu (samopraćenje), kao i u smislu provjere koju provode vanjska nadzorna tijela, poput tijela za zaštitu podataka. U skladu s člankom 25. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, u automatiziranim sustavima obrade trebali bi se bilježiti zapisi barem za sljedeće postupke obrade: prikupljanje, izmjene, obavljanje uvida, otkrivanje, uključujući prijenose, kombiniranje i brisanje. Nadalje, zapisi o obavljanju uvida i otkrivanju trebaju omogućivati utvrđivanje obrazloženja, datuma i vremena takvih postupaka te, ako je to moguće, identitet osobe koja je obavila uvid ili otkrila osobne podatke i identitet primatelja takvih osobnih podataka. Nadalje, u kontekstu sustavâ za prepoznavanje lica preporučuje se bilježenje zapisa za sljedeće dodatne postupke obrade (djelomično izvan okvira članka 25. Direktive o zaštiti podataka pri izvršavanju zakonodavstva):

- promjene referentne baze podataka (dodavanje, brisanje ili ažuriranje). Zapis bi trebao sadržavati primjerak relevantnog (dodanog, izbrisanog ili ažuriranog) prikaza ako nije moguće provjeriti zakonitost ili ishod postupaka obrade na neki drugi način

- pokušaje identifikacije ili provjere, uključujući ishod i ocjenu pouzdanosti. Trebalo bi primjenjivati strogo načelo minimizacije kako bi se u zapisima čuvala samo identifikacijska oznaka prikaza iz referentne baze podataka umjesto pohrane referentnog prikaza. Treba izbjegavati bilježenje ulaznih biometrijskih podataka, osim ako za time postoji potreba (npr. samo u slučajevima podudaranja)

- identifikacijsku oznaku korisnika koji je zatražio pokušaj identifikacije ili provjere

- svi osobni podatci pohranjeni u zapisima sustava podliježu strogim ograničenjima svrhe (revizijama) i ne bi se trebali upotrebljavati u druge svrhe (odnosno, kako bi se i dalje moglo provoditi prepoznavanje/provjeru, uključujući prikaz koji je izbrisan iz referentnih baza podataka). Potrebno je primijeniti sigurnosne mjere kako bi se osigurala cjelovitost zapisâ, dok se za otkrivanje zlouporabe zapisâ preporučuju sustavi za automatsko praćenje. Kod zapisa referentnih baza podataka, sigurnosne mjere trebale bi biti istovjetne referentnoj bazi podataka u slučaju pohrane prikazâ lica. Nadalje, trebalo bi provesti automatske postupke kojima se osigurava provedba razdoblja zadržavanja podataka za zapise.

3.2.5.6 Članak 4. stavak 4. Odgovornost

102. Voditelj obrade mora moći dokazati usklađenost obrade s načelima članka 4. stavaka od 1. do 3. Direktive o zaštiti podataka pri izvršavanju zakonodavstva, usp. članak 4. stavak 4. te Direktive. U tom pogledu ključni su sustavna i ažurna dokumentacija sustava (uključujući ažuriranja, nadogradnje i algoritamsko uvježbavanje), tehničke i organizacijske mjere (uključujući praćenje učinkovitosti sustava i potencijalne ljudske intervencije) te obrada osobnih podataka. Kako bi se dokazala zakonitost obrade, posebno važan element jest bilježenje zapisa u skladu s člankom 25. Direktive o zaštiti podataka pri izvršavanju zakonodavstva (usp. odjeljak 3.2.5.5.). Načelo odgovornosti ne odnosi se samo na sustav i obradu, nego i na dokumentiranje postupovnih jamstava, kao što su procjena nužnosti i proporcionalnosti, procjena učinka na zaštitu podataka te interna savjetovanja (npr. odobrenje rukovodstva za projekt ili interne odluke o rezultatima ocjene pouzdanosti) te vanjska savjetovanja (npr. s tijelom za zaštitu podataka). Prilog II. sadržava niz elemenata u tom pogledu.

3.2.5.7 Članak 47. Učinkoviti nadzor

103. Učinkovit nadzor nadležnih tijela za zaštitu podataka jedno je od najvažnijih postupovnih jamstava za temeljna prava i slobode pojedinaca na koje utječe primjena tehnologije prepoznavanja lica. Istodobno osiguravanje potrebnih ljudskih, tehničkih i financijskih resursa, prostorija i infrastrukture za svako tijelo za zaštitu podataka predstavlja nužan preduvjet je za djelotvorno obavljanje njegovih zadataka i

izvršavanje njegovih ovlasti[66]. Vještine stručnjaka, koji bi trebali obuhvaćati vrlo širok raspon pitanja, od kaznenih istraga i policijske suradnje do analize velikih količina podataka i umjetne inteligencije, važniji su od broja članova osoblja. Stoga bi države članice trebale osigurati da su resursi nadzornih tijela primjereni i dostatni kako bi im se omogućilo da ispune svoje ovlasti za zaštitu prava ispitanika i da pomno prate sve promjene u tom pogledu.[67]

4 ZAKLJUČAK

104. Upotreba tehnologija prepoznavanja lica neodvojivo je povezana s obradom velikih količina osobnih podataka, uključujući posebne kategorije podataka. Lice i biometrijski podatci općenito trajno su i neizbrisivo povezani s identitetom osobe. Stoga upotreba tehnologije prepoznavanja lica izravno ili neizravno utječe na brojna temeljna prava i slobode sadržane u Povelji EU-a o temeljnim pravima koja su šira od prava na privatnost i zaštitu podataka, te obuhvaćaju ljudsko dostojanstvo, slobodu kretanja, slobodu okupljanja i slično, što je osobito važno u području izvršavanja zakonodavstva i kaznenog pravosuđa.

105. EDPB razumije potrebu za time da tijela za izvršavanje zakonodavstva imaju na raspolaganju najbolje moguće alate za brzo otkrivanje identiteta počinitelja terorističkih djela i drugih teških kaznenih djela. Međutim, takvi bi se alati trebali upotrebljavati u strogoj sukladnosti s primjenjivim pravnim okvirom i samo u slučajevima kada ispunjavaju zahtjeve nužnosti i proporcionalnosti, kako je utvrđeno u članku 52. stavku 1. Povelje. Nadalje, iako suvremene tehnologije mogu biti dio rješenja, nipošto ne predstavljaju „čudotvorno rješenje".

106. Postoje određeni slučajevi upotrebe tehnologija prepoznavanja lica koji predstavljaju neprihvatljivo visok rizik za pojedince i društvo („granica neprihvatljivog"). Zbog toga su EDPB i EDPS pozvali na njihovu opću zabranu[68].

107. Drugim riječima, daljinska biometrijska identifikacija pojedinaca u javno dostupnim prostorima predstavlja visok rizik od zadiranja u privatni život pojedinaca i za nju nema mjesta u demokratskom društvu jer po svojoj prirodi podrazumijeva masovni nadzor. EDPB također smatra da sustavi za prepoznavanje lica utemeljeni na umjetnoj inteligenciji kojima se pojedinci na osnovu njihovih biometrijskih podataka kategoriziraju u skupine na temelju etničke pripadnosti, roda, kao i političke ili seksualne orijentacije nisu u skladu s Poveljom. Nadalje, EDPB je uvjeren da je upotreba tehnologije prepoznavanja lica ili sličnih tehnologija za izvođenje zaključaka o emocijama pojedinaca vrlo nepoželjna i da bi je trebalo zabraniti, uz nekoliko propisno opravdanih iznimki, kad god je to primjenjivo. Osim toga, EDPB smatra da obrada osobnih podataka u kontekstu izvršavanja zakonodavstva koja bi se temeljila na bazi podataka popunjenoj masovno i neselektivno prikupljenim osobnim podatcima, primjerice, „struganjem ekrana" za ekstrakciju fotografija i prikaza lica dostupnih na internetu, osobito onih dostupnih putem društvenih mreža, kao takva ne bi ispunila strogi zahtjev nužnosti predviđen pravom Unije.

[66] Vidjeti Komunikaciju Komisije „Prvo izvješće o primjeni i funkcioniranju Direktive o zaštiti podataka pri izvršavanju zakonodavstva (EU) 2016/680", COM(2022) 364 final, str. 3.4.1.

[67] Vidjeti Doprinos EDPB-a procjeni Direktive o zaštiti podataka pri izvršavanju zakonodavstva koju provodi Europska komisija u skladu s člankom 62. stavkom 14., https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Vidjeti Zajedničko mišljenje EDPB-a I EDPS-a 5/2021 o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

5 PRILOZI

Prilog I.: Predložak za opis scenarijâ

Prilog II.: Praktične smjernice za upravljanje projektima tehnologije prepoznavanja lica u okviru tijela za izvršavanje zakonodavstva

Prilog III.: Praktični primjeri

PRILOG I. – PREDLOŽAK ZA OPIS SCENARIJÂ

(S informacijskim okvirima za aspekte obuhvaćene scenarijem)

Opis obrade:

- Opis obrade, kontekst (povezanost s kriminalom), svrha

Izvor informacija:

- Vrsta ispitanika: ☐ svi građani ☐ osuđenici ☐ osumnjičenici ☐ djeca ☐ drugi ranjivi ispitanici
- Izvor slike: ☐ javno dostupni prostori ☐ internet ☐ privatni subjekt ☐ druge osobe ☐ drugo .....
- Povezanost s kaznenim djelom: ☐ Izravna vremenska ☐ Neizravna vremenska ☐ Izravna zemljopisna ☐ Neizravna zemljopisna ☐ Nije nužno
- Način prikupljanja informacija: ☐ na daljinu ☐ u kabini ili kontroliranom okruženju
- Kontekst – utjecaj na druga temeljna prava:
  ☐ Ne
  Da, konkretno na ☐ slobodu okupljanja
  ☐ slobodu govora
  ☐ razno:.....
- Mogućnosti za dodatne izvore informacija o ispitaniku:
  ☐ Identifikacijska isprava ☐ upotreba telefonske govornice ☐ registarska pločica vozila
  ☐ ostalo .....

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☐ baze podataka opće namjene ☐ posebne baze podataka koje se odnose na kriminalitet
- Opis načina na koji su te referentne baze podataka popunjene (i pravna osnova)
- Promjena svrhe baze podataka (npr. primarni cilj bio je sigurnost privatnog vlasništva): ☐ DA ☐ NE

Algoritam:

- Vrsta obrade: ☐ provjera usporedbom dvaju uzoraka (autentifikacija)☐ identifikacija usporedbom više uzoraka
- Razmatranja u pogledu točnosti
- Tehnička postupovna jamstva

Ishod:

- Utjecaj ☐ Izravan (npr. ispitanik može biti uhićen, ispitan, diskriminatorno postupanje)

☐Neizravan (upotrebljava se za statističke modele, ne dolazi do pokretanja ozbiljnih pravnih postupaka protiv ispitanika)

- Automatizirana odluka: ☐ DA☐ NE
- Trajanje pohrane

Pravna analiza:

- Analiza nužnosti i proporcionalnosti – svrha/težina kaznenog djela/broj osoba koje nisu uključene u obradu podataka, ali na koje ta obrada utječe
- Vrsta prethodne obavijesti ispitaniku: ☐ Pri ulasku u određeno područje
  ☐ Na mrežnom mjestu tijela za izvršavanje zakonodavstva općenito
  ☐ Na mrežnom mjestu tijela za izvršavanje zakonodavstva za konkretnu obradu
  ☐ Ostalo .....
- Mjerodavan pravni okvir:

☐ Direktiva o zaštiti podataka pri izvršavanju zakonodavstva uglavnom je prenesena u nacionalno pravo

☐ Opće odredbe nacionalnog zakonodavstva on načinu na koji tijelâ za izvršavanje zakonodavstva trebaju upotrebljavati biometrijske podatke

☐ Posebno nacionalno zakonodavstvo za tu obradu (prepoznavanje lica) mjerodavno za to nadležno tijelo

☐ Posebno nacionalno zakonodavstvo za tu obradu (automatizirana odluka)

Zaključak:

Opća razmatranja o tome je li opisana obrada vjerojatno u skladu s pravom EU-a (i određene naznake o nužnim pravnim preduvjetima)

PRILOG II. – PRAKTIČNE SMJERNICE ZA UPRAVLJANJE PROJEKTIMA TEHNOLOGIJE PREPOZNAVANJA LICA U OKVIRU TIJELA ZA IZVRŠAVANJE ZAKONODAVSTVA

U ovom se Prilogu navode dodatne praktične smjernice za tijela za izvršavanje zakonodavstva koja namjeravaju pokrenuti projekt s tehnologijom prepoznavanja lica. Sadržava daljnje informacije o organizacijskim i tehničkim mjerama koje je potrebno razmotriti tijekom uvođenja projekta i ne bi se trebao smatrati iscrpnim popisom koraka/mjera koje treba poduzeti. Prilog također treba čitati u vezi sa Smjernicama EDPB 3/2019 o obradi osobnih podataka putem videouređaja[69] i svim propisima EU-a/EGP-a i smjernicama EDPB-a o upotrebi umjetne inteligencije.

U ovom se Prilogu navode smjernice na temelju pretpostavke da će tijela za izvršavanje zakonodavstva nabavljati tehnologiju prepoznavanja lica (kao gotove proizvode). Ako tijelo za izvršavanje zakonodavstva planira razviti tehnologiju prepoznavanja lica (odnosno provesti daljnje uvježbavanje tehnologije), primjenjuju se dodatni zahtjevi za odabir potrebnih skupova podataka za uvježbavanje, validaciju i testiranje koji će se upotrebljavati tijekom razvoja, kao i uloge/mjere za razvojno okruženje. Slično tome, može biti potrebna daljnja prilagodba gotovog proizvoda za predviđenu uporabu. U tom bi slučaju trebali biti ispunjeni prethodno navedeni zahtjevi za odabir skupova podataka za testiranje, validaciju i uvježbavanje.

Pripadnost istom tijelu za izvršavanje zakonodavstva sama po sebi ne omogućuje potpuni pristup biometrijskim podatcima. Kao i kod svih drugih kategorija osobnih podataka, biometrijski podatci prikupljeni za određenu svrhu u području izvršavanja zakonodavstva na temelju posebne pravne osnove ne mogu se bez odgovarajuće pravne osnove upotrebljavati za drugu svrhu kaznenog progona (članak 4. stavak 2. Direktive (EU) 2016/680) (Direktiva o zaštiti podataka pri izvršavanju zakonodavstva)). Nadalje, razvoj/uvježbavanje alata tehnologije prepoznavanja lica smatra se drugom svrhom i treba procijeniti je li obrada biometrijskih podataka u svrhu mjerenja učinkovitosti/uvježbavanja tehnologije kako bi se izbjegao učinak na ispitanike zbog niske učinkovitosti nužna i razmjerna, uzimajući u obzir početnu svrhu obrade.

1. ULOGE I ODGOVORNOSTI

Kada tijelo za izvršavanje zakonodavstva upotrebljava tehnologije prepoznavanja lica za izvršavanje svojih zadataka obuhvaćenih područjem primjene Direktive o zaštiti podataka pri izvršavanju zakonodavstva (suzbijanje, istraga, otkrivanje ili progon kaznenih djela itd., u skladu s člankom 3. Direktive), može se smatrati voditeljem obrade za tehnologiju prepoznavanja lica. Međutim, tijela za izvršavanje zakonodavstva sastoje se od nekoliko jedinica/odjela koji mogu biti uključeni u tu obradu, na način da definiraju postupak primjene tehnologije prepoznavanja lica ili da je primjenjuju u praksi. Zbog posebnosti te tehnologije možda će biti potrebno uključiti različite jedinice kako bi se podržalo mjerenje njezine učinkovitosti ili provela dodatna obuka o tehnologiji.

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

U okviru projekta koji uključuje tehnologiju prepoznavanja lica postoji nekoliko dionika[70] unutar tijela za izvršavanje zakonodavstva koji će možda trebati biti uključeni:

- Najviše rukovodstvo – odobrava projekt nakon ocjenjivanja rizika u odnosu na potencijalne koristi.
- Službenik za zaštitu podataka i/ili pravni odjel tijela za izvršavanje zakonodavstva – pruža pomoć pri procjeni zakonitosti provedbe određenog projekta povezanog s tehnologijom prepoznavanja lica, osigurava pomoć u provedbi procjene učinka na zaštitu podataka kao i poštovanje i ostvarivanje prava ispitanika.
- Osoba odgovorna za postupak – djeluje kao posebna jedinica u okviru nadležnog tijela za izvršavanje zakonodavstva u svrhu razvoja projekta, odlučuje o pojedinostima projekta povezanog s tehnologijom prepoznavanja lica, uključujući zahtjeve u pogledu učinkovitosti sustava; odlučuje o odgovarajućem mjerenju pravednosti; utvrđuje ocjenu pouzdanosti[71]; utvrđuje prihvatljive pragove za pristranost; utvrđuje potencijalne rizike koje projekt povezan s tehnologijom prepoznavanja lica predstavlja za prava i slobode pojedinaca (na način da se savjetuje sa službenikom za zaštitu podataka i s Odjelom za umjetnu inteligenciju i/ili podatkovnu znanost (vidjeti u nastavku)) te ih predstavlja najvišem rukovodstvu. Prije donošenja odluke o pojedinostima projekta povezanog s tehnologijom prepoznavanja lica, osoba odgovorna za postupak također će se savjetovati s voditeljem referentne baze podataka kako bi razumjela svrhu upotrebe referentne baze podataka, ali i njezine tehničke pojedinosti. U slučaju ponovnog uvježbavanja nabavljene tehnologije prepoznavanja lica, osoba odgovorna za postupak također će biti zadužena za odabir skupa podataka za uvježbavanje. Kao jedinica zadužena za razvoj i odlučivanje o pojedinostima projekta, osoba odgovorna za postupak zadužena je za provedbu procjene učinka na zaštitu podataka.
- Odjel za umjetnu inteligenciju i/ili podatkovnu znanost – pomaže u provedbi procjene učinka na zaštitu podataka; objašnjava dostupne parametre za mjerenje rezultata sustava, pravednosti[72] i potencijalne pristranosti sustava; primjenjuje tehnologiju i tehnička postupovna jamstva kako bi se spriječio neovlašten pristup prikupljenim podatcima, kibernapadi i sl. U slučaju ponovnog uvježbavanja nabavljene tehnologije prepoznavanja lica, odjel za umjetnu inteligenciju ili odjel za podatkovnu znanost osposobit će sustav na temelju skupa podataka za uvježbavanje koji pruža osoba odgovorna za postupak. Taj će odjel također biti zadužen za uspostavu mjera za ublažavanje rizika koje su zajednički utvrdile osobe odgovorne za postupak (npr. rizici specifični za umjetnu inteligenciju, kao što su napadi u svrhu primjerenog zaključivanja).
- Krajnji korisnici (kao što su policijski službenici na terenu ili u forenzičkim laboratorijima) – vrše usporedbu s bazom podataka; kritički preispituju rezultate, uzimajući u obzir prethodne dokaze i pružaju povratne informacije osobi odgovornoj za postupak u pogledu lažno pozitivnih rezultata i naznaka moguće diskriminacije.
- Voditelj referentne baze podataka – posebna jedinica unutar nadležnog tijela za izvršavanje zakonodavstva zadužena za popunjavanje i upravljanje referentnom bazom podataka odnosno za baze podataka s kojom će se uspoređivati slike, uključujući brisanje prikaza lica nakon utvrđenog razdoblja čuvanja. Takva baza podataka može se izraditi posebno za predviđeni projekt povezan s

[70] Uloge navedene u nastavku indikativne su za različite dionike i njihove odgovornosti u projektu povezanom s tehnologijom prepoznavanja lica. Iako jezik koji se upotrebljava za opisivanje uloga u ovom Prilogu nije presudan, svako tijelo nadležno za izvršavanje zakonodavstva treba definirati i dodijeliti slične uloge u skladu sa svojom organizacijom. Može se dogoditi da jedinica ima više uloga, primjerice odgovornu osobu za postupak i voditelja referentne baze podataka ili osobu odgovornu za postupak i Odjel za umjetnu inteligenciju i/ili podatkovnu znanost (u slučaju da jedinica osobe odgovorne za postupak ima sva potrebna tehnička znanja).

[71] Ocjena pouzdanosti jest razina pouzdanosti predviđanja (podudaranja) u obliku vjerojatnosti. Primjerice, usporedbom dvaju predložaka postoji 90 %-tna sigurnost da oni pripadaju istoj osobi. Ocjena pouzdanosti razlikuje se od rezultata tehnologije prepoznavanja lica, međutim utječe na rezultate. Što je prag pouzdanosti veći, to je manji broj lažno pozitivnih i lažno negativnih rezultata u rezultatima tehnologije prepoznavanja lica.

[72] Pravednost se može definirati kao nedostatak nepoštene ili nezakonite diskriminacije, kao što je predrasuda na temelju rodne ili rasne pripadnosti.

tehnologijom prepoznavanja lica ili može biti uspostavljena prije pokretanja projekta za potrebe usporedbe. Voditelj referentne baze podataka zadužen je za definiranje kada se i u kojim okolnostima prikazi lica mogu pohranjivati te za utvrđivanje zahtjeva u pogledu zadržavanja podataka (u skladu s vremenom ili drugim kriterijima).

Budući da većina slučajeva uvođenja i uporabe tehnologije prepoznavanja lica predstavlja intrinzično visoki rizik za prava i slobode ispitanika, nadzorno tijelo za zaštitu podataka također bi trebalo biti uključeno u kontekstu prethodnog savjetovanja propisano člankom 28. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

2. OSMIŠLJAVANJE PRIJE NABAVE SUSTAVA TEHNOLOGIJE PREPOZNAVANJA LICA

Osoba odgovorna za postupak u okviru tijela za izvršavanje zakonodavstva prvo bi trebala jasno razumjeti postupke za primjenu tehnologije prepoznavanja lica (slučaj(evi) upotrebe) i osigurati postojanje pravne osnove za predviđeni slučaj upotrebe. Na temelju toga mora:

- Službeno opisati slučaj upotrebe. Potrebno je opisati problem koji treba riješiti i način na koji će tehnologija prepoznavanja lica pružiti rješenje, kao i pregled postupka (zadatka) u kojem će se primijeniti. U tom bi pogledu tijela za izvršavanje zakonodavstva trebala dokumentirati barem sljedeće[73]:
  - kategorije osobnih podataka zabilježenih u postupku
  - ciljeve i konkretne svrhe za koje će se upotrebljavati tehnologija prepoznavanja lica, uključujući moguće posljedice za ispitanika nakon podudaranja
  - kada i kako će se prikupljati prikazi lica (uključujući informacije o kontekstu tog prikupljanja, primjerice na ulazu u zračnu luku, putem videozapisa sa sigurnosnih kamera izvan trgovine u kojoj je počinjeno kazneno djelo i sl., te kategorije ispitanika čiji će se biometrijski podatci obrađivati)
  - bazu podataka s kojom će se usporediti slike (referentna baza podataka), kao i informacije o načinu na koji je uspostavljena, njezinoj veličini i kvaliteti biometrijskih podataka koje sadržava
  - sudjelujuća tijela za izvršavanje zakonodavstva koja će biti ovlaštena upotrebljavati sustav tehnologije prepoznavanja lica i djelovati u skladu s njime u kontekstu izvršavanja zakonodavstva (njihove profile i prava pristupa mora definirati osoba odgovorna za postupak)
  - predviđeno razdoblje zadržavanja ulaznih podataka ili trenutak koji će odrediti kraj tog razdoblja (kao što su zatvaranje ili okončanje kaznenog postupka u skladu s nacionalnim postupovnim pravom za koji su prvotno prikupljeni), kao i sve naknadne radnje (brisanje tih podataka, anonimizacija i uporaba u statističke ili istraživačke svrhe i sl.)
  - bilježenje zapisa o provedbi te dostupnost zapisa i evidencija koje se vode
  - parametre učinkovitosti (npr. točnost, preciznost, odziv, ocjena F1) i njihove minimalne prihvatljive pragove[74]

[73] U Prilogu I. naveden je popis elemenata koji voditelju obrade pomažu u opisu slučaja upotrebe tehnologije prepoznavanja lica.

[74] Postoje različiti parametri za procjenu učinkovitosti sustava tehnologije prepoznavanja lica. Svaki pokazatelj daje drukčiji pogled na rezultate sustava, a njegov uspjeh u pružanju odgovarajuće slike o tome postiže li sustav tehnologije prepoznavanja lica dobre rezultate ili ne ovisi o slučaju upotrebe tehnologije. Ako je naglasak na postizanju visokih postotaka ispravnog podudaranja lica, mogli bi se upotrijebiti parametri kao što su preciznost i odziv. Međutim, tim se parametrima ne mjeri koliko dobro tehnologija prepoznavanja lica postupa s negativnim

- procjenu koliki će broj osoba biti predmet tehnologije prepoznavanja lica u određenom vremenskom razdoblju/prilici.

- Provesti procjenu nužnosti i proporcionalnosti[75]. Činjenica da ta tehnologija postoji ne bi trebala biti pokretač njezine primjene. Osoba odgovorna za postupak prvo mora procijeniti postoji li odgovarajuća pravna osnova za predviđenu obradu. U tu se svrhu potrebno savjetovati sa službenikom za zaštitu podataka i pravnom službom. Pokretač uvođenja tehnologije prepoznavanja lica trebala bi biti činjenica da ta tehnologija predstavlja nužno i razmjerno rješenje za posebno definiran problem tijela za izvršavanje zakonodavstva. To je potrebno procijeniti u skladu sa svrhom/težinom kaznenog djela / brojem osoba koje nisu uključene, ali na koje utječe sustav tehnologije prepoznavanja lica. Za ocjenjivanje zakonitosti treba uzeti u obzir barem sljedeće: Direktivu o zaštiti podataka pri izvršavanju zakonodavstva[76], OUZP[77], [78] bilo koji postojeći pravni okvir o umjetnoj inteligenciji[79] i sve popratne smjernice koje izdaju nadzorna tijela za zaštitu podataka (kao što su smjernice EDPB-a 3/2019 o obradi osobnih podataka putem videouređaja[80]). Te zakonodavne akte EU-a uvijek bi trebalo potkrijepiti primjenjivim nacionalnim propisima, osobito u području kaznenog postupovnog prava. Procjenom proporcionalnosti trebala bi se utvrditi temeljna prava ispitanika koja bi mogla biti zahvaćena (osim privatnosti i zaštite podataka). Također treba opisati i razmotriti sve granične vrijednosti (ili nedostatak graničnih vrijednosti) utvrđene u slučaju upotrebe sustava tehnologije prepoznavanja lica. Primjerice, hoće li se sustav primjenjivati na trajnoj ili privremenoj osnovi te hoće li biti ograničen na određeno zemljopisno područje.
- Provesti procjenu učinka na zaštitu podataka [81]. Budući da bi uvođenje tehnologije prepoznavanja lica u području izvršavanja zakonodavstva moglo predstavljati visoki rizik za prava i slobode pojedinaca, potrebno je provesti procjenu učinka na zaštitu podataka[82]. Procjena učinka na zaštitu

primjerima (za koliko je njih sustav dao pogrešno podudaranje). Osoba odgovorna za postupak, uz podršku odjela za umjetnu inteligenciju i odjela za podatkovnu znanost, trebala bi moći utvrditi zahtjeve u pogledu uspješnosti i potom ih izraziti upotrebom najprikladnijih parametara u skladu sa slučajem upotrebe tehnologije prepoznavanja lica.

[75] Mogu se razmotriti daljnji koraci za osiguravanje nužnosti u pogledu prilagodbe i upotrebe sustava, što znači da se opis slučaja upotrebe može neznatno promijeniti tijekom procjene nužnosti i proporcionalnosti.

[76] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.

[77] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka.

[78] U slučajevima u kojima bi u okviru znanstvenog projekta usmjerenog na istraživanje upotrebe tehnologije prepoznavanja lica bilo potrebno obrađivati osobne podatke, pri čemu takva obrada ne bi bila obuhvaćena člankom 4. stavkom 3. Direktive o zaštiti podataka izvršavanju zakonodavstva, općenito bi se primjenjivao OUZP (članak 9. stavak 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva). U slučaju pilot-projekata nakon kojih bi uslijedile operacije izvršavanja zakonodavstva, i dalje bi bila primjenjiva Direktiva o zaštiti podataka pri izvršavanju zakonodavstva.

[79] Primjerice, postoji prijedlog Uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije, no još nije usvojen.

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

[81] Dodatne smjernice o procjenama učinka na zaštitu podataka dostupne su u sljedećim dokumentima: Smjernice za procjenu učinka na zaštitu podataka i utvrđivanje je li „vjerojatno da će obrada predstavljati visoki rizik" za potrebe Uredbe 2016/679, WP 248 rev.01, dostupno na: https://ec.europa.eu/newsroom/article29/items/611236 i Skup alata EDPS-a o odgovornosti na terenu, II. dio, dostupno na: https://edps.europa.eu/node/4582_en

[82] Ovisno o slučaju upotrebe, tehnologija prepoznavanja lica može biti obuhvaćena sljedećim kriterijima za pokretanje obrade koja predstavlja visok rizik (iz Smjernica o procjeni učinka na zaštitu podataka, WP 248 rev.01):

podataka trebala bi sadržavati sljedeće: opći opis predviđenih postupaka obrade[83], procjenu rizika za prava i slobode ispitanika[84], mjere predviđene za otklanjanje tih rizika, postupovna jamstva, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje usklađenosti. Procjena učinka na zaštitu podataka kontinuirani je postupak, zbog čega treba dodati sve nove elemente obrade i ažurirati procjenu rizika u svakoj fazi projekta.

- Potrebno je ishoditi odobrenje najvišeg rukovodstva na temelju objašnjenja rizika za prava i slobode ispitanika (iz slučaja upotrebe i tehnologije) i odgovarajućih planova za postupanje s rizicima.

3. TIJEKOM NABAVE I PRIJE UVOĐENJA TEHNOLOGIJE PREPOZNAVANJA LICA

- Donošenje odluke o kriterijima za odabir tehnologije prepoznavanja lica (algoritam). Osoba odgovorna za postupak treba odlučiti o kriterijima za odabir algoritma uz pomoć odjela za umjetnu inteligenciju i/ili odjela za podatkovnu znanost. U praksi bi to uključivalo pokazatelje pravednosti i uspješnosti o kojima je odlučeno u opisu slučaja upotrebe. Takvi kriteriji također bi trebali uključivati informacije koje se odnose na podatke upotrijebljene za uvježbavanje algoritma. Kako bi se smanjila pristranost, skup podataka za uvježbavanje, testiranje i validaciju mora u dovoljnoj mjeri uključivati uzorke svih obilježja ispitanika koji će biti predmet tehnologije prepoznavanja lica (primjerice, treba uzeti u obzir dob, spol i rasu). Pružatelj tehnologije prepoznavanja lica treba pružiti informacije i parametre o skupovima podataka za uvježbavanje, testiranje i validaciju tehnologije prepoznavanja lica te opisati mjere poduzete za mjerenje i ublažavanje učinaka moguće nezakonite diskriminacije i pristranosti. Ako je to moguće, osoba odgovorna za postupak mora provjeriti je li postojala pravna osnova na temelju koje je pružatelj tehnologije mogao upotrebljavati taj skup podataka za potrebe uvježbavanja algoritama (na temelju informacija koje će pružatelj staviti na raspolaganje). Osim toga, osoba odgovorna za postupak treba osigurati da pružatelj tehnologije prepoznavanja lica primjenjuje sigurnosne norme povezane s biometrijskim podatcima, kao što je ISO/IEC 24745, navedene u smjernicama za zaštitu biometrijskih podataka u skladu s različitim zahtjevima u pogledu povjerljivosti, cjelovitosti i obnovljivosti/opoziva tijekom pohrane i prijenosa, kao i zahtjeve i smjernice za sigurno upravljanje biometrijskim informacijama i njihovu obradu u skladu s načelima zaštite privatnosti.

- Ponovno uvježbavanje algoritma (ako je potrebno) Osoba odgovorna za postupak treba osigurati da je ugađanje sustava tehnologije prepoznavanja lica u svrhu postizanja veće točnosti prije nego što se on upotrijebi također dio nabavljenih usluga. Ako je potrebno dodatno uvježbavanje nabavljenog sustava tehnologije prepoznavanja lica kako bi se ispunili parametri točnosti, osoba odgovorna za postupak, osim donošenja odluke o ponovnom uvježbavanju sustava, uz pomoć odjela za umjetnu inteligenciju i/ili odjela za podatkovnu znanost, mora odlučiti o odgovarajućem, reprezentativnom skupu podataka koji će se upotrebljavati te provjeriti zakonitost te upotrebe podataka.

---

sustavno praćenje, opsežna obrada podataka, podudarajući ili kombinirani skupovi podataka, inovativna uporaba ili primjena novih tehnoloških ili organizacijskih rješenja.

[83] Opis obrade, kao i procjena nužnosti i proporcionalnosti, kako je opisano u prethodnim koracima, također su dio procjene učinka na zaštitu podataka, osim sâme procjene rizika. Ako je to potrebno, u procjeni učinka na zaštitu podataka bit će naveden detaljniji opis tokova osobnih podataka.

[84] Analiza rizika za ispitanike trebala bi uključivati rizike povezane s mjestom prikaza lica koje treba usporediti (lokalno/udaljeno), rizike povezane s izvršiteljima/podizvršiteljima obrade, kao i rizike specifične za strojno učenje, kada se ono primjenjuje (npr. onečišćenje podataka, neprijateljski napadi).

- Uspostava odgovarajućih postupovnih jamstava za postupanje s rizicima povezanima sa sigurnošću, pristranošću i smanjenom sposobnošću To uključuje uspostavu postupka praćenja tehnologije prepoznavanja lica nakon njezina puštanja u rad (zapisivanje i povratne informacije u svrhu točnosti i pravednosti rezultata). Osim toga, potrebno je osigurati utvrđivanje, mjerenje i ublažavanje rizika specifičnih za određene sustave strojnog učenja i tehnologije prepoznavanja lica (npr. onečišćenje podataka, neprijateljski primjeri, inverzija modela, napadi u svrhu primjerenog zaključivanja u slučaju testiranja metodom bijele kutije). Osoba odgovorna za postupak također treba uspostaviti odgovarajuća postupovna jamstva kako bi se osiguralo poštovanje zahtjeva za zadržavanje podataka za biometrijske podatke uključene u skup podataka za ponovno uvježbavanje.
- Dokumentiranje sustava tehnologije prepoznavanja lica Taj postupak treba uključivati opći opis sustava tehnologije prepoznavanja lica, detaljan opis elemenata sustava tehnologije prepoznavanja lica i postupka njegove uspostave, detaljne informacije o praćenju, funkcioniranju i kontroli sustava tehnologije prepoznavanja lica te detaljan opis povezanih rizika i mjera ublažavanja. Elementi uključeni u ovo dokumentiranje trebaju uključivati glavne elemente opisa sustava tehnologije prepoznavanja lica iz prethodnih faza (vidjeti prethodno navedeno), no poboljšat će se zahvaljujući informacijama povezanima s praćenjem uspješnosti i primjenom promjena u sustavu, uključujući sva ažuriranja verzija i/ili ponovno uvježbavanje.
- Izrada priručnika za korisnike u kojima se objašnjavaju tehnologija i slučajevi upotrebe U priručnicima moraju biti jasno objašnjeni svi scenariji i nužni preduvjeti u skladu s kojima će se upotrebljavati tehnologija prepoznavanja lica.
- Obuka krajnjih korisnika o korištenju tehnologije. U okviru takve obuke nužno je objasniti sposobnosti i ograničenja tehnologije kako bi korisnici mogli razumjeti okolnosti u kojima ju je potrebno primijeniti i slučajeve u kojima može biti netočna. Takva će obuka također doprinijeti ublažavanju rizika koji se odnose na neprovjeravanje/kritiziranje ishoda algoritma.
- Savjetovanje s nadzornim tijelom za zaštitu podataka, u skladu s člankom 28. stavkom 1. točkom (b) Direktive o zaštiti podataka pri izvršavanju zakonodavstva Pružanje informacija u skladu s člankom 13. Direktive o zaštiti podataka pri izvršavanju zakonodavstva kako bi se ispitanike obavijestilo o obradi i njihovim pravima Te obavijesti moraju biti upućene ispitanicima na odgovarajućem jeziku kako bi mogli razumjeti obradu, u kojima moraju biti objašnjeni osnovni elementi tehnologije, uključujući stope točnosti, skupove podataka za uvježbavanje i mjere poduzete za izbjegavanje diskriminacije i niske točnosti algoritma.

4. PREPORUKE NAKON UVOĐENJA TEHNOLOGIJE PREPOZNAVANJA LICA

- Osiguranje ljudske intervencije i nadzora nad rezultatima Nikada nemojte poduzimati mjere koje se odnose na pojedinca isključivo na temelju ishoda tehnologije prepoznavanja lica (to bi podrazumijevalo kršenje članka 11. Direktive o zaštiti podataka pri izvršavanju zakonodavstva – automatizirano pojedinačno donošenje odluka koje proizvodi negativne pravne učinke za ispitanika ili na njega znatno utječe). Službenik tijela za izvršavanje zakonodavstva uvijek mora preispitati rezultate dobivene tehnologijom prepoznavanja lica. Također je potrebno osigurati da korisnici u okviru tijela za izvršavanje zakonodavstva izbjegavaju automatizacijsku pristranost istraživanjem proturječnih informacija i kritičkim osporavanjem rezultata tehnologije. U tu je svrhu važna kontinuirana obuka i razvoj svijesti krajnjih korisnika. Najviše rukovodstvo trebalo bi osigurati dostupnost odgovarajućih ljudskih resursa za provedbu učinkovitog nadzora, što podrazumijeva osiguravanje dovoljno vremena svakom djelatniku da kritički razmotri rezultate tehnologije. Potrebno je zabilježiti, izmjeriti i procijeniti u kojoj mjeri ljudski nadzor mijenja prvotnu odluku donesenu na temelju tehnologije prepoznavanja lica.

- Praćenje i rješavanje pomaka modela tehnologije prepoznavanja lica (smanjenje učinkovitosti) nakon puštanja modela u uporabu
- Uspostava postupka za redovitu ponovnu procjenu rizika i sigurnosnih mjera svaki put kada dođe do promjena u pogledu tehnologije ili slučaja upotrebe
- Dokumentiranje svake promjene sustava tijekom njegova životnog ciklusa (npr. nadogradnja, ponovno uvježbavanje)
- Uspostava postupka i povezanih tehničkih sposobnosti za rješavanje zahtjeva za pristup koje podnose ispitanici Prije bilo kakvog zahtjeva mora biti uspostavljena tehnička sposobnost za izvlačenje podataka ako postoji potreba da ih se pruži ispitanicima.
- Uspostava postupaka u slučaju povrede podataka Ako dođe do povrede osobnih podataka koja uključuje biometrijske podatke, rizici će vjerojatno biti visoki. U tom slučaju svi uključeni korisnici trebaju biti upoznati s relevantnim postupcima koje treba slijediti, potrebno je o tome odmah obavijestiti službenika za zaštitu podataka kao i ispitanike.

PRILOG III. – PRAKTIČNI PRIMJERI

Postoji mnogo različitih praktičnih okruženja i svrha upotrebe prepoznavanja lica, primjerice u kontroliranim okruženjima kao što su granični prijelazi, unakrsna provjera usporedbom podataka iz policijskih baza podataka ili osobnih podataka koje je očito objavio ispitanik, sadržaj kamere koji se emitira u stvarnom vremenu (prepoznavanje lica u stvarnom vremenu) i sl. Kao rezultat toga, rizici za zaštitu osobnih podataka i drugih temeljnih prava i sloboda uvelike se razlikuju u različitim slučajevima upotrebe. Kako bi se olakšala procjena nužnosti i proporcionalnosti koja bi trebala prethoditi odluci o mogućem uvođenju prepoznavanja lica, ove Smjernice navode neiscrpan popis mogućih primjena tehnologije prepoznavanja lica u području izvršavanja zakonodavstva.

Predstavljeni i procijenjeni scenariji temelje se na **hipotetskim** situacijama, a njihova je svrha prikaz određene konkretne upotrebe tehnologije prepoznavanje lica i pomoć pri razmatranju pojedinačnih slučajeva te postavljanje općeg okvira. Nisu iscrpni i njima se ne dovode u pitanje aktualni ili budući postupci koje poduzima nacionalno nadzorno tijelo u vezi s osmišljavanjem, eksperimentiranjem ili primjenom tehnologija prepoznavanja lica. Predstavljanje tih scenarija trebalo bi služiti samo kao primjer smjernica za tvorce politika, zakonodavce i tijela za izvršavanje zakonodavstva navedenih u ovom dokumentu prilikom osmišljavanja i predviđanja provedbe tehnologija prepoznavanja lica kako bi se osigurala potpuna usklađenost s pravnom stečevinom EU-a u području zaštite osobnih podataka. U tom kontekstu valja imati na umu da čak i u sličnim situacijama upotrebe tehnologije prepoznavanja lica, prisutnost ili nepostojanje određenih elemenata može dovesti do drukčijeg ishoda procjene nužnosti i proporcionalnosti.

1 1. SCENARIJ

1.1. Opis

Sustav automatizirane granične kontrole koji omogućuje automatizirani prelazak granice autentifikacijom biometrijskog prikaza pohranjenog u elektroničkoj putnoj ispravi građana EU-a i drugih putnika koji prolaze kroz granični prijelaz i utvrđivanjem da je putnik zakoniti nositelj isprave.

Takva provjera/autentifikacija uključuje samo prepoznavanje lica usporedbom dvaju uzoraka i provodi se u kontroliranom okruženju (npr. na e-vratima zračne luke). Biometrijski podatci putnika koji prelazi granicu bilježe se kada je taj putnik izričito pozvan da pogleda u kameru na e-vratima i uspoređuju se s biometrijskim podatcima iz predočene isprave (putovnice, osobne iskaznice itd.), koja se izdaje u skladu s posebnim tehničkim zahtjevima.

Istodobno, iako obrada u takvim slučajevima u načelu nije obuhvaćena područjem primjene Direktive o zaštiti podataka pri izvršavanju zakonodavstva, ishod provjere također se može upotrijebiti za uspoređivanje (alfanumeričkih) podataka osobe s bazama podataka tijela za izvršavanje zakonodavstva u okviru nadzora državne granice i stoga može uključivati mjere sa znatnim pravnim učinkom za ispitanika, npr. uhićenje na temelju upozorenja u SIS-u. U posebnim okolnostima biometrijski podatci također se mogu upotrebljavati za pretraživanje baza podataka tijela za izvršavanje zakonodavstva radi dobivanja rezultata (u takvom bi se slučaju u ovom koraku provela identifikacija usporedbom više uzoraka).

Ishod obrade biometrijskog prikaza izravno utječe na ispitanika jer je prelazak granice moguć samo u slučaju uspješne provjere. U slučaju neuspješne identifikacije, službenici graničnog nadzora moraju provesti drugu provjeru kako bi provjerili razlikuje li se ispitanik od onog prikazanog u identifikacijskoj ispravi.

U slučaju da se aktivira upozorenje u SIS-u ili u nacionalnom sustavu , granični policajci trebaju provesti drugu provjeru i potrebne daljnje provjere, a zatim poduzeti sve potrebne mjere, npr. uhititi osobu ili obavijestiti mjerodavna nadležna tijela.

Izvor informacija:

- Vrsta ispitanika: ☒ svi pojedinci koji prelaze granice
- Izvor slike: ☒ ostalo (identifikacijska isprava)
- Povezanost s kaznenim djelom: ☒ nije nužna
- Način prikupljanja informacija: ☒ u kabini ili u kontroliranom okruženju
- Kontekst – utjecaj na druga temeljna prava: da, konkretno: ☒ pravo na slobodu kretanja
  ☒ pravo na azil

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☒ posebne baze podataka povezane s nadzorom državne granice

Algoritam:

- Vrsta provjere: ☒ provjera usporedbom dvaju uzoraka (autentifikacija)

Ishod:

- Utjecaj ☒ Izravan (ispitaniku je dopušten ili uskraćen ulazak)
- Automatizirana odluka: ☒ da

1.2. Mjerodavan pravni okvir:

U skladu s Uredbom Vijeća (EZ) br. 2252/2004[85], od 2004. putovnice i druge putne isprave koje izdaju države članice moraju sadržavati biometrijski prikaz lica pohranjen na elektroničkom čipu ugrađenom u dokument.

Zakonikom o [š]engenskim granicama[86] utvrđuju se zahtjevi za granične kontrole osoba na vanjskim granicama. Za građane EU-a i druge osobe s pravom na slobodno kretanje u skladu s pravom Unije, minimalne provjere trebale bi se sastojati od provjere njihovih putnih isprava, prema potrebi upotrebom tehničkih uređaja. Zakonik o [š]engenskim granicama naknadno je izmijenjen Uredbom (EU) 2017/2225[87], kojom su među ostalim uvedene definicije za „e-vrata", „sustav automatizirane granične kontrole" i „samoposlužni sustav", kao i mogućnost obrade biometrijskih podataka za provedbu graničnih kontrola.

Stoga se može pretpostaviti da postoji jasna i predvidljiva pravna osnova kojom se dopušta taj oblik obrade osobnih podataka. Nadalje, pravni okvir donesen je na razini Unije i izravno se primjenjuje na države članice.

1.3. Nužnost i proporcionalnost – svrha/težina kaznenog djela

Provjera identiteta građanâ EU-a u okviru automatizirane granične kontrole s pomoću biometrijskog prikaza njihova lica element je granične kontrole na vanjskim granicama EU-a. Stoga je izravno povezana sa sigurnošću granica i služi cilju od općeg interesa koji priznaje Unija. Osim toga, vrata za automatsku graničnu kontrolu doprinose bržoj obradi putnika i smanjuju rizik od ljudske pogreške. Nadalje, područje primjene, opseg i intenzitet zadiranja u prava u ovom su scenariju mnogo ograničeniji u usporedbi s drugim oblicima prepoznavanja lica. Međutim, obradom biometrijskih

[85] Uredba Vijeća (EZ) br. 2252/2004 od 13. prosinca 2004. o standardima za sigurnosna obilježja i biometrijske podatke u putovnicama i putnim ispravama koje izdaju države članice.
[86] Uredba (EU) 2016/399 Europskog parlamenta i Vijeća od 9. ožujka 2016. o Zakoniku Unije o pravilima kojima se uređuje kretanje osoba preko granica (Zakonik o [š]engenskim granicama).
[87] Uredba (EU) 2017/2225 Europskog parlamenta i Vijeća od 30. studenoga 2017. o izmjeni Uredbe (EU) 2016/399 u pogledu korištenja sustavom ulaska/izlaska.

podataka stvaraju se dodatni rizici za ispitanike, koje nadležno tijelo koje uvodi tehnologiju prepoznavanja lica i upotrebljava je treba riješiti i ograničiti na odgovarajući način.

1.4. Zaključak

Provjera identiteta građana EU-a u kontekstu automatizirane granične kontrole nužna je i razmjerna mjera, pod uvjetom da su uspostavljena odgovarajuća postupovna jamstva, osobito primjena načela ograničenja svrhe, kvalitete podataka, transparentnosti i visoke razine sigurnosti.

2 2. SCENARIJ

2.1. Opis

Tijela za izvršavanje zakonodavstva uspostavila su sustav identifikacije djece žrtava otmice. Ovlašteni policijski službenik može provesti usporedbu biometrijskih podataka djeteta za koje se sumnja da je oteto s bazom podataka djece žrtava otmice pod strogim uvjetima, isključivo u svrhu identifikacije maloljetnika koji mogu odgovarati opisu nestalog djeteta za koje je pokrenuta istraga i izdano upozorenje.

Predmetna obrada obuhvaća usporedbu lica ili slike pojedinca, koji bi mogli odgovarati opisu nestalog djeteta, sa slikama pohranjenima u bazi podataka. Takva bi se obrada trebala odvijati u posebnim slučajevima, a ne na sustavnoj osnovi.

Baza podataka na temelju koje će se primijeniti usporedba popunjena je slikama nestale djece za koju je prijavljena sumnja na otmicu, prijetnja životu djeteta ili njegovu fizičkom integritetu te je pokrenuta kaznena istraga u okviru pravosudnog tijela i izdano je upozorenje o otmici djeteta. podatci se prikupljaju u okviru postupaka koje je utvrdilo nadležno tijelo za izvršavanje zakonodavstva, odnosno policijski službenici ovlašteni za provođenje pravosudnih policijskih operacija. Kategorije osobnih podataka koji se bilježe jesu:

- identitet, nadimak, pseudonim, roditelji, državljanstvo, adrese, e-adrese, telefonski brojevi
- datum i mjesto rođenja
- informacije o roditeljima
- fotografija s tehničkim značajkama koje omogućuju uporabu uređaja za prepoznavanje lica i druge fotografije.

Rezultate usporedbe također mora pregledati i provjeriti ovlašteni službenik kako bi se prethodni dokazi potkrijepili rezultatima usporedbe i te isključili mogući lažno pozitivni rezultati.

Slike i osobni podatci djece smiju se zadržati samo tijekom trajanja upozorenja i moraju se izbrisati odmah nakon zaključenja ili okončanja kaznenog postupka u skladu s nacionalnim postupcima za koje su uneseni u bazu podataka.

Iako se razdoblje zadržavanja biometrijskih podataka u bazi podataka može predvidjeti na relativno dugo razdoblje i definirati u skladu s nacionalnim pravom, ostvarivanje prava ispitanika, osobito pravo na ispravak i brisanje, osigurava dodatno jamstvo za ograničavanje zadiranja u pravo na zaštitu osobnih podataka dotičnih ispitanika.

Izvor informacija:

- Vrsta ispitanika: ☒ djeca
- Izvor slike ☒ ostalo: nije unaprijed definirano, sumnja se da je ispitanik dijete žrtva otmice
- Povezanost s kaznenim djelom ☒ neizravna vremenska ☒ neizravna zemljopisna
- Način prikupljanja informacija: ☒ u kabini ili u kontroliranom okruženju
- Kontekst: utjecaj na druga temeljna prava ☒ da, kako slijedi: ☒ razno

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost ☒ određena baza podataka

Algoritam:

- Vrsta provjere: ☒ identifikacija usporedbom više uzoraka

Ishod:

- Utjecaj ☒ izravan
- Automatizirana odluka: ☒ NE, obvezno preispitivanje koje provodi ovlašteni službenik

Pravna analiza:

- Mjerodavan pravni okvir: ☒ posebno nacionalno pravo za ovu obradu (prepoznavanje lica)

2.2. Mjerodavan pravni okvir:

Nacionalnim pravom predviđen je poseban pravni okvir za uspostavu baze podataka, kojim se utvrđuju svrhe obrade i kriteriji za popunjavanje baze podataka, pristup toj bazi podataka i njezinu upotrebu. Zakonodavnim mjerama potrebnima za njegovu provedbu također je predviđeno utvrđivanje razdoblja zadržavanja, kao i upućivanje na primjenjiva načela integriteta i povjerljivosti. Zakonodavnim mjerama također se predviđaju načini pružanja informacija ispitaniku te, u ovom slučaju, jednom ili nositelju roditeljske odgovornosti, kao i ostvarivanje prava ispitanika i moguće ograničenje, ako je primjenjivo. Tijekom izrade prijedloga odgovarajuće zakonodavne mjere bilo je nužno provesti savjetovanje s nacionalnim nadzornim tijelom.

2.3. Nužnost i proporcionalnost – svrha/težina kaznenog djela te broj osoba koje nisu uključene u obradu podataka, ali na koje ta obrada utječe

Uvjeti i postupovna jamstva za obradu

Ovlašteni službenik može provesti usporedbu na temelju prepoznavanja lica samo kao krajnju mjeru, osim ako nisu dostupna druga manje invazivna sredstva te ako je to strogo potrebno, primjerice u slučaju sumnje u vjerodostojnost osobne isprave maloljetnika koji putuje i/ili nakon pregleda prethodnih prikupljenih dokaza i materijala koji upućuju na moguće podudaranje s opisom nestalog djeteta za koje se provodi kaznena istraga.

Također je osigurano je dodatno postupovno jamstvo na način da rezultate usporedbe na temelju prepoznavanja lica obvezno mora preispitati i potvrditi ovlašteni službenik kako bi se prethodni dokazi potkrijepili rezultatima usporedbe te da isključe mogući lažni pozitivni rezultati.

Cilj koji se želi postići

Uspostava baze podataka služi važnim ciljevima od općeg javnog interesa, posebno sprečavanju, istrazi, otkrivanju ili progonu kaznenih djela ili izvršavanju kaznenopravnih sankcija te zaštiti prava i sloboda drugih. Čini se da uspostava baze podataka i predviđena obrada doprinose identifikaciji otete djece te se stoga mogu smatrati prikladnom mjerom za doprinos legitimnom cilju istrage i kaznenog progona takvih kaznenih djela.

Svrha i sadržaj baze podataka

Svrhe obrade jasno su definirane zakonom, a baza podataka smije se koristiti samo u svrhu identificiranja nestale djece za koju je prijavljena sumnja na otmicu djeteta i pokrenuta kaznena istraga pod nadzorom pravosudnog tijela te za koju je izdano upozorenje za otmicu djeteta. Zakonom utvrđeni uvjeti u pogledu sadržaja baze podataka usmjereni su na strogo ograničavanje broja ispitanika i osobnih podataka koji će biti uključeni u bazu podataka. Nositelja roditeljske odgovornosti nad djetetom mora se obavijestiti o poduzetoj obradi i uvjetima za ostvarivanje prava njegova djeteta u vezi s biometrijskom obradom predviđenom za potrebe identifikacije ili osobnim podatcima djeteta pohranjenima u bazi podataka.

2.4. Zaključak

S obzirom na nužnost i proporcionalnost obrade koja je predviđena te najbolji interes djeteta za provedbu takve obrade osobnih podataka i pod uvjetom da su uspostavljena dovoljna jamstva kako bi se posebno osiguralo ostvarivanje prava ispitanika, osobito uzimajući u obzir činjenicu da će se obrađivati podatci djece, takva se primjena obrade na temelju prepoznavanja lica može smatrati vjerojatno usklađenom s pravom EU-a.

Nadalje, u pogledu vrste obrade i korištene tehnologije, koja predstavlja visok rizik za prava i slobode predmetnih ispitanika, EDPB smatra da izrada prijedloga zakonodavne mjere koju donosi nacionalni parlament ili regulatorne mjere koja se temelji na takvoj zakonodavnoj mjeri i koja se odnosi na obradu, mora uključivati prethodno savjetovanje s nadzornim tijelom kako bi se osigurala dosljednost i usklađenost s primjenjivim pravnim okvirom, usp. članak 28. stavak 2. Direktive o zaštiti podataka pri izvršavanju zakonodavstva.

3 3. SCENARIJ

3.1. Opis

Tijekom policijskih intervencija u neredima i posljedičnih istraga, određeni broj osoba identificiran je u svojstvu osumnjičenika, npr. prethodnim istragama u kojima je upotrijebljen sadržaj snimljen videonadzorom (CCTV, tj. televizija zatvorenog kruga) ili na temelju iskaza svjedoka. Slike tih osumnjičenika uspoređuju se sa slikama osoba snimljenih videonadzorom ili mobilnim uređajima na mjestu zločina ili u okolnim područjima.

Kako bi pribavila detaljnije dokaze o osobama za koje se sumnja da su sudjelovale u neredima tijekom prosvjeda, policija izrađuje bazu podataka koja se sastoji od prikazâ s djelomičnom lokalnom i vremenskom povezanošću s neredima. Baza podataka uključuje privatne snimke koje su policiji prenijeli građani, materijale snimljene videonadzorom u javnom prijevozu, materijal za videonadzor u vlasništvu policije te materijal koji objavljuju mediji bez posebnih ograničenja ili postupovnih jamstava. Prikazivanje teških oblika kriminaliteta nije nužan preduvjet za prikupljanje datoteka u bazi podataka. Stoga se osobe koje nisu sudjelovale u neredima, odnosno značajan postotak lokalnog stanovništva koje se zateklo na licu mjesta u trenutku prosvjeda ili je sudjelovalo u prosvjedu, ali ne i u neredima, pohranjuju u bazu podataka. Riječ je o tisućama videozapisa i slikovnih datoteka.

S pomoću softvera za prepoznavanje lica svim se licima koja se pojavljuju u tim datotekama dodjeljuje jedinstvena identifikacijska oznaka lica. Lica pojedinačnih osumnjičenika zatim se automatski uspoređuju s tim identifikacijskim oznakama. Baza podataka koja se sastoji od svih biometrijskih predložaka u tisućama videozapisa i slika pohranjuje se do završetka svih mogućih istraga. Pozitivne rezultate rješavaju nadležni službenici, koji odlučuju o daljnjim koracima. To može uključivati

pridruživanje datoteke pronađene u bazi podataka kaznenom dosjeu dotične osobe te daljnje mjere, kao što su ispitivanje ili uhićenje te osobe.

Nacionalnim pravom predviđena je opća odredba prema kojoj je obrada biometrijskih podataka u svrhu jedinstvene identifikacije fizičke osobe dopuštena ako je to strogo nužno te podložno odgovarajućim postupovnim jamstvima za prava i slobode dotične osobe.

Izvor informacija:

- Vrsta ispitanika: ☒ sve osobe
- Izvor slike: ☒ javno dostupni prostori ☒ privatni subjekt ☒ druge osobe ☒ ostalo: mediji
- Povezanost s kaznenim djelom: ☒ izravna zemljopisna ili vremenska povezanost nužno ne postoji
- Način prikupljanja informacija: ☒ na daljinu
- Kontekst – utjecaj na druga temeljna prava: da, konkretno na ☒ kontekst slobode okupljanja
- Dostupni dodatni izvori informacija o ispitaniku:
  ☒ ostalo: nije isključeno (kao što je upotreba bankomata ili trgovine u koje je osoba ušla) jer se na temelju slika ne može provesti kontrola motiva

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☒ posebne baze podataka povezane s područjem kriminala

Algoritam:

- Vrsta obrade: ☒ identifikacija usporedbom više uzoraka

Ishod:

- Utjecaj: ☒ Izravan (npr. ispitanik može biti uhićen ili ispitan)
- Automatizirana odluka: ☒ NE
- Trajanje pohrane: do završetka svih mogućih istraga

Pravna analiza:

- Vrsta prethodne obavijesti ispitaniku: ☒ Na mrežnom mjestu tijela za izvršavanje zakonodavstva općenito
- Mjerodavan pravni okvir: ☒ Direktiva o zaštiti podataka pri izvršavanju zakonodavstva uglavnom je prenesena u nacionalno pravo ☒ Opće odredbe nacionalnog zakonodavstva o načinu na koji tijelâ za izvršavanje zakonodavstva trebaju upotrebljavati biometrijske podatke

3.2. Mjerodavan pravni okvir:

Kako je prethodno pojašnjeno, pravne osnove kojima se samo ponavlja opća klauzula članka 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva nisu dovoljno jasne i njima se pojedincima ne pruža dovoljno jasan uvid u uvjete i okolnosti u kojima su tijela za izvršavanje zakonodavstva ovlaštena upotrebljavati snimke videonadzora s javnih prostora u svrhu izrade biometrijskog predloška njihova lica i uspoređivati ih s policijskim bazama podataka, drugim dostupnim snimkama videonadzora ili privatnim snimkama itd. Pravni okvir utvrđen u ovom scenariju stoga ne ispunjava minimalne zahtjeve nužne da bi služio kao pravna osnova.

3.3. Nužnost i proporcionalnost

U ovom primjeru obrada izaziva različitu zabrinutost u pogledu načela nužnosti i proporcionalnosti iz nekoliko razloga:

Osobe nisu osumnjičene za teško kazneno djelo. Prikazivanje teških oblika kriminaliteta nije nužan preduvjet za uporabu datoteka u bazi podataka koja sadržava slikovni materijal. Nadalje, izravna vremenska i zemljopisna povezanost s kaznenim djelom nije nužan preduvjet za upotrebu datoteka u bazi podataka, što dovodi do pohranjivanja velikog postotka lokalnog stanovništva u biometrijsku bazu podataka na razdoblje od potencijalno nekoliko godina, do završetka svih istražnih postupaka.

Baza podataka mjesta zločina nije ograničena na prikaze koje ispunjavaju zahtjeve proporcionalnosti, što dovodi do neograničene količine prikaza koji se mogu upotrijebiti u svrhu usporedbe, što je protivno načelu smanjenja količine podataka. Manja količina prikaza također bi omogućila razmatranje nealgoritamskih i manje invazivnih sredstava, npr. super-prepoznavača.[88]

Budući da je primjer uzet iz okruženja prosvjeda, vjerojatno je da prikazi otkrivaju politička mišljenja sudionika u prosvjedima, što je druga posebna kategorija podataka na koju bi taj scenarij mogao utjecati. U ovom scenariju nije jasno kako se prikupljanje tih podataka može spriječiti te kojim postupovnim jamstvima. Nadalje, ako ispitanici saznaju da je njihovo sudjelovanje u prosvjedu dovelo do njihova unosa u biometrijsku policijsku bazu podataka, to može imati ozbiljne negativne učinke na njihovo buduće ostvarivanje prava na okupljanje.

Biometrijski predlošci u bazi podataka također se mogu međusobno uspoređivati. Time se policiji omogućuje ne samo da traži određenu osobu u svim svojim materijalima, nego i da uspostavi obrazac ponašanja osobe tijekom razdoblja od nekoliko dana. Također može prikupiti dodatne informacije o osobama kao što su društveni kontakti i politička uključenost.

Zadiranje u prava dodatno se pojačava činjenicom da se podatci obrađuju bez znanja ispitanika.

Imajući na umu da osobe cijelo vrijeme snimaju fotografije i videozapise te da se čak i sveprisutna pokrivenost videonadzorom može analizirati u biometrijskom smislu, to može dovesti do ozbiljnih odvraćajućih učinaka.

Opsežna uporaba privatnih fotografija i videozapisa, uključujući potencijalnu zlouporabu kao što je prijavljivanje osobe policiji, još je jedan razlog za zabrinutost. Budući da zlouporaba poput prijavljivanja osobe predstavlja rizik svojstven kaznenom postupku općenito, rizik je znatno veći u pogledu prilagodljivosti obrađenih podataka i broja uključenih osoba, s obzirom na to da osobe također mogu prenijeti materijale koji se odnose na određenu osobu ili skupinu osoba koje im nisu drage. Zahtjevi policije za učitavanje fotografija i videozapisa mogu potencijalno imati vrlo niske pragove u pogledu materijala, posebno jer je to moguće učiniti anonimno ili barem bez dolaska u policijsku postaju i identificiranjem.

3.4. Zaključak

U ovom primjeru ne postoji posebna zakonska odredba koja bi mogla služiti kao pravna osnova. Međutim, čak i da postoji dostatna pravna osnova, ne bi bili ispunjeni zahtjevi u pogledu nužnosti i

[88] Riječ je o osobama s izvanrednom sposobnošću prepoznavanja lica. Usp. također: *Face Recognition by Metropolitan Police Super-Recognisers* (Prepoznavanje lica koje vrše super-prepoznavači u sklopu metropolitanske policije), 26. veljače 2016., DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

proporcionalnosti, što bi dovelo do nerazmjernog zadiranja u prava ispitanika na poštovanje privatnog života i zaštitu osobnih podataka u skladu s Poveljom.

4 4. SCENARIJ

4.1. Opis

Policija provodi način identificiranja osumnjičenika koji su počinili teško kazneno djelo snimljenih na videonadzoru retrospektivnom tehnologijom prepoznavanja lica. Službenik ručno odabire prikaz(e) osumnjičenika u videomaterijalu koji je prikupljen s mjesta zločina ili drugdje u okviru preliminarne istrage, a prikaz(e) potom šalje forenzičkom odjelu. Forenzički odjel upotrebljava tehnologiju prepoznavanja lica kako bi te prikaze povezao s prikazima pojedinaca koje je policija prethodno prikupila u bazi podataka (takozvana baza podataka s opisima, koja se sastoji od osumnjičenika i bivših osuđenika). Baza podataka s opisima za taj postupak, privremeno i u izoliranom okruženju, analizira se primjenom tehnologije prepoznavanja lica kako bi se moglo provesti traženje podudaranja. Kako bi se smanjilo zadiranje u prava i interese osoba za koje se dobiju rezultati, vrlo ograničen broj zaposlenika forenzičke službe ima dopuštenje provesti stvaran postupak traženja podudaranja. Pristup podatcima ograničen je na službenike kojima je povjeren određeni predmet te se provodi ručna kontrola rezultata prije prosljeđivanja bilo kakvih rezultata istražnom službeniku. Biometrijski podatci ne prosljeđuju se izvan kontroliranog, izoliranog okruženja. U daljnjoj istrazi upotrebljavaju se samo rezultat i slika (a ne biometrijski predložak). Zaposlenici prolaze posebnu obuku o pravilima i postupcima za takvu obradu, a svaka obrada osobnih i biometrijskih podataka dostatno je utvrđena u nacionalnom pravu.

Izvor informacija:

- Vrsta ispitanika: ☒ osumnjičenici identificirani na temelji snimki videonadzora
- Izvor slike: ☒ javno dostupni prostori ☒ internet
- Povezanost s kaznenim djelom: ☒ Izravna vremenska
  ☒ Izravna zemljopisna
- Način prikupljanja informacija: ☒ na daljinu
- Kontekst – utjecaj na druga temeljna prava: da, konkretno na: ☒ slobodu okupljanja ☒ slobodu govora ☒ razno: __

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☒ posebne baze podataka povezane s područjem kriminala

Algoritam:

- Vrsta obrade: ☒ identifikacija usporedbom više uzoraka

Ishod:

- Utjecaj:☒ izravan (npr. ispitanik je uhićen, ispitan)
- Automatizirana odluka: ☒ NE

Pravna analiza:

- Mjerodavan pravni okvir: ☒ Posebno nacionalno pravo za tu obradu (prepoznavanje lica) za to nadležno tijelo

4.2. Mjerodavan pravni okvir:

U ovom je scenariju u nacionalnom pravu utvrđeno da se biometrijski podatci mogu upotrebljavati u provedbi forenzičke analize kada je to strogo potrebno za postizanje svrhe identifikacije osumnjičenika koji su počinili teško kazneno djelo na temelju podudaranja slika u bazi podataka s opisom. U nacionalnom pravu navodi se koji se podatci mogu obrađivati, kao i postupci za očuvanje cjelovitosti i povjerljivosti osobnih podataka i postupci za njihovo uništavanje, čime se osiguravaju dostatna jamstva protiv rizika od zlouporabe i proizvoljnosti.

4.3. Nužnost i proporcionalnost

Upotreba prepoznavanja lica očito je vremenski učinkovitija od ručnog traženja rezultata na forenzičkoj razini. Prethodnim ručnim odabirom prikazâ ograničava se zadiranje u prava u usporedbi s uporabom svih videomaterijala u bazi podataka, čime se razlikuju i ciljaju samo osobe obuhvaćene ciljem borbe protiv teških kaznenih djela. Međutim, i dalje je važno razmotriti može li se traženje rezultata podudaranja provesti ručno u razumnom roku, ovisno o pojedinačnom predmetu. Ograničenjem osoba s pristupom tehnologiji i osobnim podatcima smanjuje se utjecaj na prava na privatnost i zaštitu podataka, kao i na biometrijske predloške koji se ne pohranjuju ili ne upotrebljavaju u naknadnoj fazi istrage. Ručna kontrola rezultata također podrazumijeva manji rizik od lažno pozitivnih rezultata.

4.4. Zaključak

Važno je da se nacionalnim zakonodavstvom osigura odgovarajuća pravna osnova za obradu biometrijskih podataka i za nacionalnu bazu podataka u odnosu na koju se provodi podudaranje. U ovom scenariju uspostavljeno je nekoliko mjera kako bi se ograničilo zadiranje u prava na zaštitu podataka, kao što su uvjeti za upotrebu tehnologije prepoznavanja lica navedeni u pravnoj osnovi, broj osoba koje imaju pristup tehnologiji i biometrijskim podatcima, ručne kontrole itd. Tehnologija prepoznavanja lica značajno poboljšava učinkovitost u istražnom radu forenzičkog odjela policije, temelji se na pravu kojim se policiji omogućuje obrada biometrijskih podataka kada je to apsolutno nužno i stoga se unutar tih ograničenja može smatrati zakonitim zadiranjem u prava pojedinca.

5 5. SCENARIJ

5.1. Opis

Daljinska biometrijska identifikacija podrazumijeva da se identiteti osoba utvrđuju s pomoću biometrijskih identifikatora (prikaz lica, hod, šarenica itd.) na daljinu, u javnom prostoru te na kontinuiranoj ili stalnoj osnovi, na način da ih se uspoređuje s (biometrijskim) podatcima pohranjenima u bazi podataka[89]. Daljinska biometrijska identifikacija provodi se u stvarnom vremenu ako se snimanje slikovnog materijala, usporedba i identifikacija odvijaju bez značajnog kašnjenja.

Prije svakog uvođenja daljinske biometrijske identifikacije u stvarnom vremenu policija sastavlja popis za praćenje subjekata od interesa u okviru istrage koji se popunjava prikazima lica pojedinaca. Na temelju obavještajnih podataka koji upućuju na to da će se pojedinci nalaziti na određenom području, kao što su trgovački centar ili javni trg, policija donosi odluku o tome kada, gdje i koliko dugo primjenjivati daljinsku biometrijsku identifikaciju.

Na dan djelovanja na teren postavljaju policijski kombi, koji upotrebljavaju kao kontrolni centar i u kojem je prisutan viši policijski službenik. U kombiju se nalaze monitori koji prikazuju snimke videonadzora snimljene kamerama smještenim u blizini, koje su postavljene na *ad hoc* osnovi ili su povezane s već postavljenim kamerama. Kada pješaci prolaze pored kamera, tehnologija izolira prikaze

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

lica, pretvara ih u biometrijski predložak i uspoređuje ih s biometrijskim predlošcima osoba na popisu za praćenje.

Ako se otkrije moguća podudarnost između popisa za praćenje i osoba koje su prošle pored kamera, šalje se upozorenje službenicima u kombiju, koji zatim savjetuju službenike na terenu ako je upozorenje pozitivno, npr. putem radiouređaja. Službenik na terenu zatim odlučuje hoće li intervenirati, pristupiti osobi ili u konačnici uhititi osobu. Mjere koje službenik poduzima na terenu evidentiraju se. U slučaju skrivene provjere prikupljene informacije (kao što je podatak s kim je osoba, što nosi i kamo ide) pohranjuju se.

Navedenim nacionalnim pravom predviđena je opća odredba prema kojoj je obrada biometrijskih podataka u svrhu jedinstvene identifikacije fizičke osobe dopuštena ako je to strogo nužno te podložno odgovarajućim postupovnim jamstvima za prava i slobode dotične osobe.

Izvor informacija:

- Vrsta ispitanika: ☒ sve osobe
- Izvor slike: ☒ javno dostupni prostori
- Povezanost s kaznenim djelom: ☒ izravna zemljopisna ili vremenska povezanost nužno ne postoji
- Način prikupljanja informacija: ☒ na daljinu
- Kontekst – utjecaj na druga temeljna prava: da, konkretno na: ☒ slobodu okupljanja ☒ slobodu govora ☒ razno
- Dostupni dodatni izvori informacija o ispitaniku:
  ☒ ostalo: nije isključeno (kao što su uporaba bankomata ili trgovine u koje je osoba ušla)

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☒ posebne baze podataka povezane s područjem kriminala

Algoritam:

- Vrsta obrade: ☒ identifikacija usporedbom više uzoraka

Ishod:

- Utjecaj: ☒ izravan (ispitanik je uhićen ili ispitan)
- Automatizirana odluka: ☒ NE
- Trajanje pohrane: do završetka svih mogućih istraga

Pravna analiza:

- Vrsta prethodne obavijesti ispitaniku: ☒ na mrežnom mjestu tijela za izvršavanje zakonodavstva općenito
- Mjerodavan pravni okvir: ☒ Direktiva o zaštiti podataka pri izvršavanju zakonodavstva uglavnom je prenesena u nacionalno pravo ☒ Opće odredbe nacionalnog zakonodavstva o načinu na koji tijelâ za izvršavanje zakonodavstva trebaju upotrebljavati biometrijske podatke

5.2. Mjerodavan pravni okvir:

Pravne osnove kojima se samo ponavlja opća klauzula članka 10. Direktive o zaštiti podataka pri izvršavanju zakonodavstva nisu dovoljno jasne i njima se pojedincima ne nudi dovoljno jasan uvid u uvjete i okolnosti u kojima su tijela za izvršavanje zakonodavstva ovlaštena upotrebljavati snimke videonadzora s javnih prostora u svrhu izrade biometrijskog predloška njihova lica i uspoređivati ih s

policijskim bazama podataka. Stoga pravni okvir utvrđen u ovom scenariju ne ispunjava minimalne zahtjeve potrebne da bi služio kao pravna osnova[90].

5.3. Nužnost i proporcionalnost

Prag u pogledu nužnosti i proporcionalnosti postaje viši što je zadiranje u prava dublje. Postoje različite posljedice daljinske biometrijske identifikacije na temeljna prava u javnim prostorima:

Scenariji podrazumijevaju praćenje svih prolaznika u odgovarajućem javnom prostoru. Stoga uvelike utječe na razumno očekivanje stanovništva da je anonimno u javnim prostorima[91]. To je nužan preduvjet za mnoge aspekte demokratskog procesa, kao što su odluke o pridruživanju građanskoj udruzi, pridruživanju skupovima i sastajanju s osobama iz svih društvenih i kulturnih sredina, sudjelovanju u političkim prosvjedima i posjećivanju mjesta svih vrsta. Pojam anonimnosti u javnim prostorima ključan je za slobodno prikupljanje i razmjenu informacija i ideja. Njime se čuva pluralizam mišljenja, sloboda mirnog okupljanja i sloboda udruživanja te zaštita manjina i podržava se načela diobe vlasti te sustav provjere i ravnoteže. Ugrožavanje anonimnosti u javnim prostorima može značajno ograničiti ponašanje građana koji će se možda suzdržati od određenog ponašanja koje je u okviru slobodnog i otvorenog društva. To bi utjecalo na javni interes jer demokratsko društvo zahtijeva samoodređenje i sudjelovanje svojih građana u demokratskom procesu.

Ako se primjenjuje takva tehnologija, jednostavno hodanje ulicom, vožnja podzemnom željeznicom ili odlazak u pekarnicu u zahvaćenom području dovest će do toga da tijela za izvršavanje zakonodavstva prikupljaju osobne podatke, uključujući biometrijske podatke, te, u prvom scenariju, do uspoređivanja s policijskim bazama podataka u svrhu traženja podudarnosti. Situacija u kojoj bi se isto učinilo uzimanjem otisaka prstiju očito bi bilo neproporcionalna.

Broj zahvaćenih ispitanika iznimno je visok jer mjera utječe na sve osobe koje se zateknu u predmetnom javnom prostoru. Nadalje, scenariji bi podrazumijevali automatiziranu masovnu obradu biometrijskih podataka i masovno uspoređivanje biometrijskih podataka s policijskim bazama podataka radi dobivanja rezultata.

U europskoj sudskoj praksi zabranjen je masovni nadzor (npr. ESLJP u predmetu S. i Marper protiv Ujedinjene Kraljevine ocijenio je neselektivno zadržavanje biometrijskih podataka „neproporcionalnim zadiranjem" u pravo na privatnost jer se ne smatra „nužnim u demokratskom društvu").

Daljinska biometrijska identifikacija toliko je podložna masovnom nadzoru da ne postoje pouzdana sredstva ograničavanja. Budući da moguća uporaba videosnimki bez biometrijske identifikacije već predstavlja značajno, ali istodobno ograničeno, zadiranje u prava, u osnovi se razlikuje od videonadzora kao takvog. S druge strane, ako se primjenjuje tehnologija prepoznavanja lica, doći će do promjene kvalitete sustava videonadzora, koji je već široko rasprostranjen kao glavni izvor podataka. Nadalje, osobito kad je riječ o impliciranim odvraćajućim učincima, moguća ograničenja u primjeni već postojećih instalacija videonadzora neće biti vidljiva, zbog čega javnost u njih neće imati povjerenja.

U okviru daljinske biometrijske identifikacije koju provode policijska tijela prema svima se postupa kao prema potencijalnom osumnjičeniku. Međutim, u državi vladavine prava smatra se da su građani nevini

[90] U slučajevima u kojima bi u okviru znanstvenog projekta usmjerenog na istraživanje upotrebe tehnologije prepoznavanja lica bilo potrebno obrađivati osobne podatke, pri čemu takva obrada ne bi bila obuhvaćena člankom 4. stavkom 3. Direktive o zaštiti podataka izvršavanju zakonodavstva ili ne bi bila obuhvaćena područjem primjene prava Unije, primjenjivao bi se OUZP. U slučaju pilot-projekata nakon kojih bi uslijedile operacije izvršavanja zakonodavstva, i dalje bi bila primjenjiva Direktiva o zaštiti podataka pri izvršavanju zakonodavstva.
[91] Odgovor EDPB-a zastupnicima u Europskom parlamentu u vezi s aplikacijom za prepoznavanje lica koju je razvio Clearview AI, 10. lipnja 2020., upućivanje: OUT2020-0052.

sve dok im se ne dokaže krivica. To se načelo djelomično odražava u Direktivi o zaštiti podataka pri izvršavanju zakonodavstva, u kojoj se naglašava potreba za razlikovanjem, u mjeri u kojoj je to moguće, između postupanja prema osuđenicima ili osumnjičenicima za kazneno djelo; u tom slučaju tijela za izvršavanje zakonodavstva moraju imati *„ozbiljn[e] razlo[ge] vjerovati da su počinile ili će počiniti kazneno djelo"* (članak 6. točka (a) Direktive o zaštiti podataka pri izvršavanju zakonodavstva) i onih koji nisu osuđeni ili osumnjičeni za kriminalnu aktivnost.

Ako se primjenjuje na prometnim čvorištima ili u javnim prostorima, pri čemu tijela za izvršavanje zakonodavstva upotrebljavaju tehnologiju kojom se može jedinstveno identificirati jedna osoba te pratiti i analizirati njezina lokacija i kretanje, otkrit će se najosjetljivije informacije o osobi (čak i seksualne preferencije, vjera, zdravstveni problemi). To predstavlja golem rizik od nezakonitog pristupa podatcima i njihove uporabe.

Postavljanje sustava koji omogućuje otkrivanje same srži ponašanja i obilježja pojedinca dovodi do snažnih odvraćajućih učinaka. Time se ljude navodi da ponovno promisle o tome hoće li se uključiti u određenu manifestaciju, čime se šteti demokratskom procesu. Susret s prijateljem za kojeg se zna da ima problema s policijom ili da se ponaša na određeni način također bi se mogao smatrati kritičnim jer bi to dovelo do privlačenja pažnje algoritma sustava, a time i tijela za izvršavanje zakonodavstva.

Nije moguće zaštititi ranjive ispitanike, kao što su djeca. Nadalje, to utječe na osobe koje imaju profesionalni interes, a često i odgovarajuću pravnu obvezu, da njihovi kontakti ostanu povjerljivi, kao što su novinari, odvjetnici i svećenstvo. To bi, primjerice, moglo dovesti do otkrivanja izvora i novinara ili do činjenice da se osoba savjetuje s braniteljem u kaznenom postupku. Problem se ne odnosi samo na nasumične javne prostore na kojima se susreću, primjerice, novinari i njihovi izvori, već i na javne prostore nužne za pristup institucijama ili stručnjacima u tom pogledu.

Nadalje, nelagoda ljudi u pogledu tehnologije prepoznavanja lica može ih dovesti do toga da promijene ponašanje, izbjegavaju mjesta na kojima se upotrebljava takva tehnologija, a time i da se povuku iz društvenog života i kulturnih događanja. Ovisno o opsegu uvođenja tehnologije prepoznavanja lica, utjecaj na ljude može biti toliko značajan da utječe na njihov dostojanstveni život[92].

Stoga postoji velika vjerojatnost da će utjecati na bit, odnosno na samu osnovu prava na zaštitu osobnih podataka. Snažni pokazatelji (usp. odjeljak 3.1.3.2. Smjernica) osobito su sljedeći: tijela za izvršavanje zakonodavstva u velikoj mjeri automatski obrađuju jedinstvene biološke značajke ljudi s pomoću algoritama koji se temelje na vjerodostojnosti, uz ograničenu objašnjivost rezultata. Ograničenja prava na privatnost i zaštitu podataka nameću se bez obzira na ponašanje osobe ili okolnosti koje se na tu osobu odnose. U statističkom pogledu gotovo svi ispitanici na koje utječe ovo zadiranje u prava pojedinci su koji poštuju zakone. Postoje samo ograničene mogućnosti pružanja informacija ispitaniku. Sudska zaštita u većini slučajeva moguća je tek naknadno.

Oslanjanje na sustav koji se temelji na vjerojatnosti i s ograničenom objašnjivošću može dovesti do raspršivanja odgovornosti i manjak pravnog lijeka te može biti poticaj za nemar.

Nakon primjene takvog sustava, koji se također može primijeniti na postojeće kamere videonadzora, uz vrlo malo napora i bez vidljivosti pojedincima, sustav se može zloupotrijebiti omogućavanjem sustavnog i brzog sastavljanja popisa osoba prema etničkom podrijetlu, spolu, vjeri i sl. Načelo obrade

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

osobnih podataka prema unaprijed utvrđenim kriterijima kao što su lokacija osobe i ruta koju je prešla već se primjenjuje[93] i podložno je diskriminaciji.

U odnosu na načela osjetljivosti, izričitosti i količine obrađenih podataka, sustavi za prepoznavanje lica na daljinu na javno dostupnim mjestima mogu se zloupotrijebiti sa štetnim učincima za dotične pojedince. Takvi se podatci također mogu lako prikupiti i zloupotrijebiti kako bi se izvršio pritisak na ključne sudionike u sustavu provjere i ravnoteže, kao što su politička oporba, službenici i novinari.

Konačno, sustavi tehnologije prepoznavanja lica često uključuju jake predrasude u pogledu rasne i rodne pripadnosti: lažno pozitivni rezultati nerazmjerno utječu na nebijelce i žene[94], što dovodi do diskriminacije. Policijske mjere koje se provode nakon lažno pozitivnog rezultata, kao što su pretresi i uhićenja, dodatno stigmatiziraju te skupine.

5.4. Zaključak

Prethodnom navedenim scenarijima koji se odnose na daljinsku obradu biometrijskih podataka u javnim prostorima za potrebe identifikacije ne postiže se pravedna ravnoteža između suprotstavljenih privatnih i javnih interesa, što predstavlja nerazmjerno zadiranje u prava ispitanika u skladu s člancima 7. i 8. Povelje.

6 6. SCENARIJ

6.1. Opis

Privatni subjekt stavlja na raspolaganje aplikaciju kojom se prikazi lica ekstrahiraju s interneta kako bi se stvorila baza podataka. Korisnik, npr. policija, zatim može učitati sliku, a aplikacija će s pomoću biometrijske identifikacije pokušati pronaći podudaranje na temelju prikaza lica ili biometrijskih predložaka u svojoj bazi podataka.

Lokalna policijska uprava provodi istragu kaznenog djela snimljenog videokamerom, pri čemu se određeni broj potencijalnih svjedoka i osumnjičenika ne može identificirati uspoređivanjem prikupljenih podataka s internim bazama podataka ili obavještajnim podatcima. Pojedinci na temelju prikupljenih informacija nisu registrirani ni u jednoj postojećoj policijskoj bazi podataka. Policija odlučuje upotrijebiti prethodno opisani alat za identifikaciju pojedinaca s pomoću biometrijske identifikacije koji nudi privatno poduzeće.

Izvor informacija:

- Vrsta ispitanika: ☒ svi građani (svjedoci) ☒ osuđenici ☒ osumnjičenici
- Izvor slike: ☒ videozapisi s javnog mjesta ili prikupljeni drugdje u okviru preliminarne istrage
- Povezanost s kaznenim djelom: ☒ nije nužna
- Način prikupljanja informacija: ☒ na daljinu

[93] Usp. članak 6. Direktive (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela i članak 33. Uredbe (EU) 2018/1240 Europskog parlamenta i Vijeća od 12. rujna 2018. o uspostavi europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) i izmjeni uredaba (EU) br. 1077/2011, (EU) br. 515/2014, (EU) 2016/399, (EU) 2016/1624 i (EU) 2017/2226.

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

- Kontekst – utjecaj na druga temeljna prava: da, konkretno na: ☒ slobodu okupljanja ☒ slobodu govora ☒ razno: __

Referentna baza podataka (s kojom se uspoređuju prikupljene informacije):

- Specifičnost: ☒ baze podataka opće namjene koje se popunjavaju podatcima s interneta

Algoritam:

- Vrsta obrade: ☒ identifikacija usporedbom više uzoraka

Ishod:

- Utjecaj ☒ izravan (npr. ispitanik je uhićen, ispitan, diskriminatorno postupanje)
- Automatizirana odluka: ☒ NE

Pravna analiza:

- Vrsta prethodne obavijesti ispitaniku: ☒ ne

6.2. Mjerodavan pravni okvir:

Ako privatni subjekt pruža uslugu koja uključuje obradu osobnih podataka za koju utvrđuje svrhu i sredstva (u ovom slučaju struganje ekrana za ekstrakciju slika s interneta za izradu baze podataka), taj privatni subjekt mora imati pravnu osnovu za takvu obradu. Nadalje, tijelo za izvršavanje zakonodavstva koje odluči upotrijebiti tu uslugu za svoje potrebe mora imati pravnu osnovu za obradu, za koju utvrđuje svrhe i sredstva. Kako bi tijelo za izvršavanje zakonodavstva moglo obrađivati biometrijske podatke, mora postojati pravni okvir kojim se utvrđuju cilj, osobni podatci koji se obrađuju, svrhe obrade i postupci za očuvanje cjelovitosti i povjerljivosti osobnih podataka te postupci za njihovo uništavanje.

Ovaj scenarij podrazumijeva masovno prikupljanje osobnih podataka pojedinaca koji nisu svjesni da se njihovi podatci prikupljaju. Takva obrada može biti zakonita samo u vrlo iznimnim okolnostima. Ovisno o tome gdje se baza podataka koja upotrebljava takvu uslugu nalazi, takva obrada može uključivati prijenos osobnih podataka i/ili posebnih kategorija osobnih podataka izvan Europske unije (što provodi policija; primjerice, „slanjem" prikaza lica iz videozapisa nadzornih kamera ili dobivenim na drugi način), a za takav su prijenos propisani posebni uvjeti (vidjeti članak 39. Direktive o zaštiti podataka pri izvršavanju zakonodavstva).

U ovom scenariju ne postoje posebna pravila kojima bi se tijelima za izvršavanje zakonodavstva omogućila ta obrada.

6.3. Nužnost i proporcionalnost

Činjenica da tijelo za izvršavanje zakonodavstva upotrebljava uslugu podrazumijeva da se osobni podatci dijele s privatnim subjektom koji upotrebljava bazu podataka u kojoj se osobni podatci prikupljaju na neograničen, masovan način. Ne postoji veza između osobnih podataka koje je prikupilo tijelo za izvršavanje zakonodavstva i cilja koji to tijelo nastoji ostvariti. Razmjena podataka između tijela za izvršavanje zakonodavstva i privatnog subjekta također podrazumijeva nedostatak kontrole nadležnog tijela nad podatcima koje obrađuje privatni subjekt, kao i velike poteškoće za ispitanike u ostvarivanju njihovih prava jer neće biti svjesni činjenice da se njihovi podatci obrađuju na taj način. Time se postavlja vrlo visok prag za situacije u kojima bi se takva obrada uopće mogla provesti. Upitno je postoji li bilo koji cilj koji bi ispunjavao zahtjeve utvrđene u Direktivi jer se sva odstupanja i ograničenja prava na privatnost i zaštitu podataka primjenjuju samo ako je to nužno potrebno. Obrada se ne može opravdati samim općim interesom učinkovitosti u borbi protiv teških kaznenih djela ako se

takve velike količine podataka prikupljaju neselektivno. Stoga ta obrada ne bi ispunjavala zahtjeve u pogledu nužnosti i proporcionalnosti.

6.4. Zaključak

Nedostatak jasnih, preciznih i predvidljivih pravila koja ispunjavaju zahtjeve iz članaka 4. i 10. Direktive te nedostatak dokaza da je ta obrada strogo nužna za postizanje predviđenih ciljeva dovode do zaključka da upotreba ove aplikacije ne bi ispunila zahtjeve nužnosti i proporcionalnosti te bi predstavljala nerazmjerno zadiranje u prava ispitanika na poštovanje privatnog života i zaštitu osobnih podataka u skladu s Poveljom.