Smernice

Smernice 05/2022 o uporabi tehnologij za prepoznavanje obraza na področju preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj

Različica 2.0

Sprejete 26. aprila 2023

Zgodovina različic

Različica 1.0	12. maj 2022	Sprejetje smernic za javno posvetovanje
Različica 2.0	26. april 2023	Sprejetje smernic po javnem posvetovanju

Vsebina

POVZETEK

Čedalje več organov kazenskega pregona uporablja ali namerava uporabljati tehnologijo za prepoznavanje obraza. Uporablja se lahko za **avtentikacijo** ali za **identifikacijo** osebe in se lahko uporablja na videoposnetkih (na primer videonadzornih sistemov CCTV) ali fotografijah. Uporablja se lahko za različne namene, med drugim za iskanje oseb na policijskih seznamih nadzorovanih oseb ali za spremljanje gibanja osebe na javni površini.

Tehnologija za prepoznavanje obraza temelji na obdelavi **biometričnih podatkov**, zato vključuje obdelavo posebnih vrst osebnih podatkov. Za to tehnologijo se pogosto uporabljajo sestavni deli **umetne inteligence** ali strojnega učenja. To resda omogoča obsežno obdelavo podatkov, vendar povzroča tudi tveganje diskriminacije in napačnih rezultatov. Ta tehnologija se lahko uporablja v nadzorovanih okoliščinah ena na ena ter za velike množice in na pomembnih prometnih vozliščih.

Tehnologija za prepoznavanje obraza je za **organe kazenskega pregona občutljivo orodje**. Ti organi so izvršni organi in imajo suverena pooblastila. Ta tehnologija morda posega v temeljne pravice – lahko celo presega pravico do varstva osebnih podatkov – ter lahko vpliva na našo socialno, demokratično in politično stabilnost.

V zvezi z varstvom osebnih podatkov v okviru preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj morajo biti izpolnjene **zahteve iz direktive o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov** (Direktiva (EU) 2016/680). V Direktivi (EU) 2016/680 je zagotovljen specifični okvir v zvezi z uporabo tehnologije za prepoznavanje obraza, zlasti v trinajstem odstavku njenega 3. člena (izraz „biometrični podatki“), 4. (načela v zvezi z obdelavo osebnih podatkov), 8. (zakonitost obdelave), 10. (obdelava posebnih vrst osebnih podatkov) in 11. členu (avtomatizirano sprejemanje posameznih odločitev).

Uporaba tehnologije za prepoznavanje obraza lahko vpliva tudi na številne druge temeljne pravice. Zato je za razlago Direktive (EU) 2016/680 ključna **Listina EU o temeljnih pravicah** (v nadaljevanju: Listina), zlasti v zvezi s pravico do varstva osebnih podatkov iz 8. člena Listine in pravice do zasebnosti iz 7. člena Listine.

Zakonodajni ukrepi, ki so pravna podlaga za obdelavo osebnih podatkov, neposredno posegajo v pravice, zagotovljene v 7. in 8. členu Listine. Obdelava biometričnih podatkov v vseh okoliščinah že sama po sebi pomeni resen poseg. To ni odvisno od rezultata, na primer pozitivnega ujemanja. Kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, mora biti predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin.

Pravna podlaga mora biti vsebinsko **dovolj jasna**, da se državljanom ustrezno pojasnijo pogoji in okoliščine, v katerih so organi pooblaščeni, da lahko uporabijo katere koli ukrepe za zbiranje podatkov in tajno opazovanje. Zgolj prenos splošne določbe iz 10. člena Direktive (EU) 2016/680 v nacionalno zakonodajo je premalo natančen in predvidljiv.

Preden nacionalni zakonodajalec oblikuje novo pravno podlago za katero koli obliko obdelave biometričnih podatkov z uporabo prepoznavanja obraza, se je treba **posvetovati** s pristojnim nadzornim organom za varstvo podatkov.

Zakonodajni ukrepi morajo biti **ustrezni** za doseganje legitimnih ciljev v skladu z zadevno zakonodajo. **Cilj v splošnem interesu**, tudi če je temeljni, sam po sebi ne more upravičiti omejevanja temeljne

pravice. Zakonodajni ukrepi bi morali **razlikovati** med osebami in biti usmerjeni na osebe, za katere veljajo, glede na cilj, na primer za boj proti specifičnemu hudemu kaznivemu dejanju. Če ukrep na splošno zajema vse osebe, tj. brez takega razlikovanja, omejitve ali izjeme, se poseg poglobi. To se zgodi tudi, kadar obdelava podatkov zajema pomemben del prebivalstva.

Podatke je treba obdelovati na način, s katerim se zagotavljata uporabnost ter učinkovitost pravil in načel EU o varstvu podatkov. Na podlagi posamezne situacije je treba pri **oceni nujnosti in sorazmernosti** opredeliti in upoštevati tudi vse možne posledice za druge temeljne pravice. Če se podatki sistematično obdelujejo brez vednosti posameznikov, na katere se nanašajo osebni podatki, lahko to vzbuja **splošni občutek stalnega nadzora**. To lahko vodi do zastraševalnih učinkov v zvezi z nekaterimi ali vsemi zadevnimi temeljnimi pravicami, kot so človekovo dostojanstvo iz 1. člena Listine, svoboda misli, vesti in vere iz 10. člena Listine, svoboda izražanja iz 11. člena Listine ter svoboda zbiranja in združevanja iz 12. člena Listine.

Obdelava posebnih vrst podatkov, kot so biometrični podatki, se lahko za **nujno potrebno** (10. člen Direktive (EU) 2016/680) šteje le, če so poseg v varstvo osebnih podatkov in njegove omejitve omejeni na to, kar je absolutno potrebno, tj. nepogrešljivo, pri čemer je izključena vsakršna splošna ali sistematična obdelava.

Dejstvo, da je posameznik, na katerega se nanašajo osebni podatki, **sam objavil** fotografijo (10. člen Direktive (EU) 2016/680), ne pomeni, da se povezani biometrični podatki, ki jih je mogoče s specifičnimi tehničnimi sredstvi pridobiti iz fotografije, štejejo za javne. Privzete nastavitve storitve, na primer da so predloge javno dostopne, ali to, da izbira ni mogoča, na primer predloge se objavijo, uporabnik pa te nastavitve ne more spremeniti, se nikakor ne bi smele razlagati kot javno objavljeni podatki.

Direktiva (EU) 2016/680 v 11. členu vzpostavlja okvir za **avtomatizirano sprejemanje posameznih odločitev**. Z uporabo tehnologije za prepoznavanje obraza se obdelujejo posebne vrste podatkov, poleg tega to lahko vodi do oblikovanja profilov, odvisno od načina in namena uporabe te tehnologije. V vsakem primeru je v skladu s pravom Unije in tretjim odstavkom 11. člena Direktive (EU) 2016/680 prepovedano oblikovanje profilov, katerega posledica je diskriminacija posameznikov na podlagi posebnih vrst osebnih podatkov.

Direktiva (EU) 2016/680 v 6. členu obravnava potrebo po razlikovanju med različnimi kategorijami posameznikov, na katere se nanašajo osebni podatki. V zvezi s posamezniki, na katere se nanašajo osebni podatki in za katere ni dokazov, na podlagi katerih bi bilo mogoče sklepati, da bi njihovo ravnanje lahko bilo povezano, četudi posredno ali oddaljeno, z legitimnim ciljem v skladu z Direktivo (EU) 2016/680, poseg najverjetneje ni upravičen.

V skladu z **načelom najmanjšega obsega podatkov** (točka e prvega odstavka 4. člena Direktive (EU) 2016/680) se zahteva še, da bi bilo treba vsa videogradiva, ki niso pomembna za namen obdelave, pred objavo vedno odstraniti ali anonimizirati (na primer z zabrisanjem, brez možnosti, da se podatki obnovijo).

Upravljavec mora skrbno proučiti, kako (oziroma ali sploh) lahko izpolni zahteve glede **pravic posameznika, na katerega se nanašajo osebni podatki**, še preden se začne kakršna koli obdelava s tehnologijo za prepoznavanje obraza, saj se s to tehnologijo pogosto obdelujejo posebne vrste osebnih podatkov, brez vsakršne očitne vključitve posameznika, na katerega se nanašajo osebni podatki.

Učinkovito uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, je odvisno od tega, ali upravljavec izpolnjuje svoje **obveznosti v zvezi z zagotavljanjem informacij** (13. člen Direktive

(EU) 2016/680). Pri presoji, ali gre za poseben primer iz drugega odstavka 13. člena Direktive (EU) 2016/680, je treba upoštevati številne dejavnike, vključno s tem, ali se osebni podatki zbirajo brez vednosti posameznika, na katerega se nanašajo osebni podatki, saj bi bil to edini način, da se posameznikom, na katere se nanašajo osebni podatki, omogoči učinkovito uresničevanje njihovih pravic. Če se odločitve sprejemajo izključno na podlagi tehnologije za prepoznavanje obraza, morajo biti posamezniki, na katere se nanašajo osebni podatki, obveščeni o značilnostih avtomatiziranega sprejemanja odločitev.

V zvezi z **zahtevami za dostop** bi moralo, kadar so biometrični podatki shranjeni in povezani z identiteto tudi z alfanumeričnimi podatki, to v skladu z načelom najmanjšega obsega podatkov pristojnemu organu omogočiti, da odobri zahtevo za dostop na podlagi iskanja po teh alfanumeričnih podatkih in brez kakršne koli dodatne obdelave biometričnih podatkov drugih oseb (tj. z iskanjem v zbirki podatkov s tehnologijo za prepoznavanje obraza).

Tveganja za posameznike, na katere se nanašajo osebni podatki, so še posebej resna, če so netočni podatki shranjeni v policijski podatkovni zbirki in/ali se delijo z drugimi subjekti. Upravljavec mora shranjene podatke in podatke v sistemih za prepoznavanje obraza ustrezno **popraviti** (glej tudi uvodno izjavo 47 Direktive (EU) 2016/680).

Pravica do **omejitve obdelave** postane še posebej pomembna v primeru uporabe tehnologije za prepoznavanje obraza (ta temelji na algoritmih, zato nikoli ne pokaže dokončnega rezultata) v primerih, v katerih se zbirajo velike količine podatkov, pri čemer se lahko točnost in kakovost identifikacije razlikujeta.

Ocena učinka v zvezi z varstvom podatkov, preden se uporabi tehnologija za prepoznavanje obraza, je obvezna zahteva, prim. 27. člen Direktive (EU) 2016/680. Evropski odbor za varstvo podatkov (EOVP) priporoča, da se rezultati takih ocen ali vsaj glavnih ugotovitev in sklepov ocene učinka v zvezi z varstvom podatkov objavijo, in sicer kot ukrep za krepitev zaupanja in preglednosti.

Večina primerov uvajanja in uporabe tehnologije za prepoznavanje obraza že sami po sebi pomenijo veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Zato bi se moral organ, ki uvaja tehnologijo za prepoznavanje obraza, še pred namestitvijo tega sistema **posvetovati** s pristojnim nadzornim organom.

Glede na edinstveno naravo biometričnih podatkov bi moral organ, ki izvaja in/ali uporablja tehnologijo za prepoznavanje obraza, posebno pozornost nameniti **varnosti obdelave** v skladu z 29. členom Direktive (EU) 2016/680. Organ kazenskega pregona bi moral zagotoviti zlasti, da je sistem skladen z ustreznimi standardi in izvaja ukrepe za zaščito biometričnih predlog. Načela varstva podatkov in zaščitni ukrepi morajo biti v tehnologijo vgrajeni, še preden se obdelava osebnih podatkov sploh začne. Zato mora organ kazenskega pregona, tudi če namerava namestiti in uporabljati tehnologijo zunanjih ponudnikov za prepoznavanje obraza, zagotoviti, na primer s postopkom javnega naročanja, da se uvede le taka tehnologija za prepoznavanje obraza, ki temelji na načelih **vgrajenega in privzetega varstva podatkov**.

Vodenje dnevnikov (prim. 25. člen Direktive (EU) 2016/680) je pomemben zaščitni ukrep za preverjanje zakonitosti obdelave, ki se izvaja interno (tj. notranje spremljanje, ki ga izvaja zadevni upravljavec oziroma obdelovalec) ali ga izvajajo zunanji nadzorni organi. V okviru sistemov za prepoznavanje obraza se vodenje dnevnikov priporoča tudi v primerih spreminjanja referenčne podatkovne zbirke ter ob poskusih identifikacije ali preverjanja, vključno s podatki o uporabniku, rezultatu in oceno zaupanja. Vendar je vodenje dnevnikov le eden od poglavitnih elementov splošnega **načela odgovornosti** (prim. četrti odstavek 4. člena Direktive (EU) 2016/680). Upravljavec mora biti

sposoben dokazati skladnost obdelave z osnovnimi načeli varstva podatkov iz prvega do tretjega odstavka 4. člena Direktive (EU) 2016/680.

EOVP opozarja na skupni **poziv**, ki ga je izdal skupaj z Evropskim nadzornikom za varstvo podatkov, k prepovedi nekaterih vrst obdelave v zvezi z (1.) biometrično identifikacijo posameznikov na daljavo na javno dostopnih mestih, (2.) sistemi za prepoznavanje obraza, ki jih podpira umetna inteligenca in ki posameznike na podlagi njihovih biometričnih podatkov razvrščajo v skupine glede na etnično pripadnost, spol, politično ali spolno usmerjenost ali druge značilnosti, ki lahko vodijo v diskriminacijo, (3.) uporabo tehnologij za prepoznavanje obraza ali podobnih tehnologij, da bi sklepali o čustvih fizične osebe ter (4.) obdelavo osebnih podatkov v okviru preprečevanja, odkrivanja preiskovanja ali pregona kaznivih dejanj, ki bi temeljila na podatkovni zbirki, v kateri bi se zbirali osebni podatki v množičnem obsegu in neselektivno, na primer s pridobivanjem podatkov s fotografij in slik obrazov, dostopnih na spletu.

Glavni zaščitni ukrep za zadevne temeljne pravice je **učinkovit nadzor**, ki ga izvajajo pristojni nadzorni organi za varstvo podatkov. Zato morajo države članice zagotoviti, da imajo nadzorni organi ustrezne in zadostne vire, ki jim omogočajo izpolnjevanje njihovih pooblastil.

Te smernice so **namenjene** zakonodajalcem na ravni EU in nacionalni ravni ter organom kazenskega pregona in njihovim uradnikom, ki izvajajo in uporabljajo sisteme za prepoznavanje obraza. Posameznikom pa so namenjene, če jih to zanima na splošno ali kot posameznike, na katere se nanašajo osebni podatki, zlasti v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki.

Namen smernic je seznanjati z nekaterimi značilnostmi tehnologije za prepoznavanje obraza in s pravnim okvirom, ki se uporablja v sklopu kazenskega pregona (zlasti v zvezi z Direktivo (EU) 2016/680).

- Poleg tega zagotavljajo **orodje za podporo pri razvrstitvi občutljivosti zadevnega primera uporabe** (Priloga I).
- Vsebujejo tudi **praktične smernice za organe kazenskega pregona, ki želijo naročiti in upravljati sistem za prepoznavanje obraza** (Priloga II).
- V smernicah so navedeni številni značilni **primeri uporabe in številni relevantni premisleki**, zlasti v zvezi s testom nujnosti in sorazmernosti (Priloga III).

1 UVOD

1. Tehnologija za prepoznavanje obraza se lahko uporablja za samodejno prepoznavanje posameznikov na podlagi njihovega obraza. Ta tehnologija pogosto temelji na umetni inteligenci, kot so tehnologije strojnega učenja. Aplikacije te tehnologije se čedalje bolj preizkušajo in uporabljajo na številnih področjih – od individualne uporabe do uporabe v zasebnih organizacijah in v javni upravi. Tudi organi kazenskega pregona od uporabe teh tehnologij pričakujejo koristi. Z njo so mogoče rešitve za razmeroma nove izzive, kot so preiskave, ki vključujejo veliko količino zajetih dokazov, in za znane težave, zlasti v zvezi s pomanjkanjem osebja za naloge opazovanja in iskanja.

2. Velik del povečanega zanimanja za tehnologijo za prepoznavanje obraza temelji na njeni učinkovitosti in nadgradljivosti. S tem so povezane tudi slabosti, ki so značilne za tehnologijo in njeno uporabo – tudi v velikem obsegu. Resda je lahko več tisoč naborov osebnih podatkov analiziranih le s pritiskom na gumb, vendar pri tem lahko že majhni učinki algoritemske diskriminacije ali napačne identifikacije povzročijo, da je zelo veliko posameznikov resno prizadetih v njihovem ravnanju in vsakdanjem življenju. Obseg obdelave osebnih podatkov, zlasti biometričnih podatkov, je še en ključni element

tehnologije za prepoznavanje obraza, saj obdelava osebnih podatkov pomeni poseg v temeljno pravico do varstva osebnih podatkov v skladu z 8. členom Listine Evropske unije o temeljnih pravicah (Listina).

3. To, da organi kazenskega pregona uporabljajo tehnologijo za prepoznavanje obraza, bo imelo (in delno že ima) pomembne posledice za posameznike in skupine ljudi, tudi za manjšine. Te posledice bodo pomembno vplivale tudi na naše skupno življenje ter na našo socialno, demokratično in politično stabilnost, pri čemer se je treba zavedati velikega pomena pluralizma in političnega nasprotovanja. Pravica do varstva osebnih podatkov je pogosto ključna kot temeljni pogoj za zagotavljanje drugih temeljnih pravic. Uporaba te tehnologije lahko pomembno posega v temeljne pravice, lahko celo presega pravico do varstva osebnih podatkov.

4. EOVP zato meni, da je pomembno prispevati k stalnemu vključevanju tehnologije za prepoznavanje obraza na področje kazenskega pregona, kot to urejata Direktiva (EU) 2016/680[1] oziroma nacionalna zakonodaja, v katero se ta prenaša, in zagotoviti te smernice. Namen smernic je zakonodajalcem na ravni EU in na nacionalni ravni ter organom kazenskega pregona in njihovim uradnikom zagotoviti ustrezne informacije, potrebne pri izvajanju in uporabi sistemov za prepoznavanje obraza. Področje uporabe smernic je omejeno na tehnologijo za prepoznavanje obraza. Ob tem lahko druge oblike obdelave osebnih podatkov na podlagi biometričnih podatkov, ki jo izvajajo organi kazenskega pregona, zlasti če obdelava poteka na daljavo, pomenijo podobna ali dodatna tveganja za posameznike, skupine in družbo. Glede na ustrezne okoliščine so lahko nekateri vidiki teh smernic koristen vir tudi v teh primerih. Nazadnje, pomembne informacije lahko pridobijo tudi posamezniki, ki jih to zanima na splošno ali kot posameznike, na katere se nanašajo osebni podatki, zlasti v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki.

5. Smernice so sestavljene iz glavnega dokumenta in treh prilog. V glavnem dokumentu sta predstavljena tehnologija in pravni okvir, ki se uporablja. V pomoč pri opredelitvi nekaterih glavnih vidikov za razvrstitev resnosti posega v temeljne pravice na zadevnem področju uporabe je v Prilogi I na voljo predloga. Organom kazenskega pregona, ki želijo naročiti in upravljati sistem za prepoznavanje obraza, pa so praktične smernice na voljo v Prilogi II. Glede na področje uporabe tehnologije za prepoznavanje obraza so lahko pomembni različni premisleki. V Prilogi III je zato na voljo sklop hipotetičnih scenarijev in ustreznih premislekov.

2 TEHNOLOGIJA

2.1 Ena biometrična tehnologija, dve različni funkciji

6. Prepoznavanje obraza je tehnologija, ki deluje na podlagi verjetnosti in lahko samodejno prepozna posameznike na podlagi njihovega obraza ter tako potrdi njihovo identiteto ali jih identificira.

7. Tehnologija za prepoznavanje obraza spada v širšo kategorijo biometrične tehnologije. Biometrija vključuje vse avtomatizirane postopke, ki se uporabljajo za prepoznavanje posameznika na podlagi kvantificiranja njegovih fizičnih, fizioloških ali vedenjskih značilnosti (prstni odtisi, struktura šarenice, glas, način hoje, vzorci krvnih žil itd.). Te značilnosti so opredeljene kot biometrični podatki, saj omogočajo ali potrjujejo edinstveno identifikacijo zadevne osebe.

[1] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.

8. To velja za obraze ljudi ali, natančneje, tehnično obdelavo slike obraza z uporabo naprav za prepoznavanje obraza: s posnetkom obraza (fotografija ali videoposnetek), kar se imenuje biometrični vzorec, je mogoče pridobiti digitalni prikaz različnih značilnosti zadevnega obraza (to se imenuje predloga).

9. Biometrična predloga je digitalni prikaz edinstvenih značilnosti, ki so bile pridobljene iz biometričnega vzorca in jih je mogoče shraniti v biometrično podatkovno zbirko[2]. Ta predloga naj bi bila edinstvena in specifična za vsako osebo, z vidika časa pa je načeloma trajna[3]. V fazi prepoznavanja naprava to predlogo primerja z drugimi predlogami, ki so bile predhodno pripravljene ali izračunane neposredno iz biometričnih vzorcev, kot so obrazi, najdeni na sliki, fotografiji ali videoposnetku. Prepoznavanje obraza je tako dvostopenjski postopek: najprej se pridobi slika obraza in se preoblikuje v predlogo, temu pa sledi prepoznavanje tega obraza s primerjavo ustrezne predloge z eno ali več drugimi predlogami.

10. Tako kot vsak biometrični postopek lahko tudi prepoznavanje obraza opravlja dve različni funkciji:

    - **avtentikacijo** osebe; cilj tega je preveriti, ali je oseba resnično tista, za katero se izdaja. V tem primeru sistem primerja vnaprej pripravljeno biometrično predlogo ali vzorec (na primer shranjeno (shranjenega) na pametni kartici ali v biometričnem potnem listu) s samo enim obrazom, na primer obrazom osebe, ki pride do kontrolne točke, da preveri, ali gre za isto osebo. Ta funkcija tako temelji na primerjavi dveh predlog. To se imenuje tudi **preverjanje** ena na ena;

    - **identifikacijo** osebe; cilj tega je, da se v skupini posameznikov na zadevnem območju na sliki ali v podatkovni zbirki poišče zadevna oseba. V tem primeru mora sistem obdelati vsak posnetek obraza, ustvariti biometrično predlogo in nato preveriti, ali se ta ujema s posnetkom osebe, katere posnetek je že v sistemu. Ta funkcija tako temelji na primerjavi ene predloge s predlogami ali vzorci v podatkovni zbirki (izhodišče). To se imenuje tudi identifikacija s primerjanjem z več vzorci. Tako lahko na primer poveže zapis osebnega imena (priimek, ime) z obrazom, če se primerjava opravi s fotografijami v podatkovni zbirki, povezanimi s priimki in imeni. To lahko vključuje tudi spremljanje osebe v množici, ne da bi to nujno pomenilo povezavo s civilno identiteto osebe.

11. V obeh primerih uporabljene tehnike za prepoznavanje obraza temeljijo na oceni ujemanja med predlogami, in sicer med primerjanimi predlogami in izhodiščem(-i). S tega vidika delujejo na podlagi verjetnosti: s primerjavo se določi večja ali manjša verjetnost, da je zadevna oseba resnično oseba, ki jo je treba avtentificirati ali identificirati; če ta verjetnost preseže določen prag v sistemu, ki ga določi uporabnik ali razvijalec sistema, bo sistem domneval, da obstaja ujemanje.

12. Čeprav sta obe funkciji – avtentikacija in identifikacija – različni, se obe nanašata na obdelavo biometričnih podatkov, povezanih z določenim ali določljivim posameznikom, in zato pomenita obdelavo osebnih podatkov in, natančneje, obdelavo posebnih vrst osebnih podatkov.

13. Prepoznavanje obraza je del širšega nabora tehnik za obdelavo videoposnetkov. Nekatere videokamere lahko snemajo ljudi na opredeljenem območju, zlasti njihove obraze, vendar jih kot takih ni mogoče uporabiti za avtomatizirano prepoznavanje posameznikov. Enako velja za preprosto fotografijo: fotoaparat ni sistem za prepoznavanje obraza, saj je treba fotografije ljudi obdelati na specifičen način, da se pridobijo biometrični podatki.

[2] Guidelines on facial recognition (Smernice o prepoznavanju obraza), Posvetovalni odbor iz Konvencije št. 108 o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Svet Evrope, junij 2021.

[3] To je lahko odvisno od vrste biometrije in starosti posameznika, na katerega se nanašajo osebni podatki.

14. Tudi zgolj zaznavanje obrazov s tako imenovanimi pametnimi kamerami ne pomeni nujno sistema za prepoznavanje obraza. Čeprav digitalne tehnike za zaznavanje neobičajnega vedenja ali nasilnih dogodkov ali za prepoznavanje čustev na obrazu ali celo silhuet odpirajo tudi pomembna vprašanja glede etike in učinkovitosti, se ne smejo šteti za biometrične sisteme, ki obdelujejo posebne vrste osebnih podatkov, če njihov cilj ni edinstvena identifikacija osebe in če obdelava osebnih podatkov ne vključuje drugih posebnih vrst osebnih podatkov. Ti primeri niso popolnoma nepovezani s prepoznavanjem obrazov in zanje še vedno veljajo pravila o varstvu osebnih podatkov[4]. Poleg tega se lahko ta vrsta sistema odkrivanja uporablja v povezavi z drugimi sistemi, katerih cilj je identifikacija osebe, zaradi česar se lahko šteje za tehnologijo za prepoznavanje obraza.

15. V nasprotju z na primer sistemi za zajemanje in obdelavo videoposnetkov, za katere je treba namestiti fizične naprave, je prepoznavanje obrazov funkcija programske opreme, ki jo je mogoče implementirati v obstoječe sisteme (kamere, podatkovne zbirke slik itd.). Taka funkcija je tako lahko povezana ali združena s številnimi sistemi in se kombinira z drugimi funkcijami. Za tako vključitev v že obstoječo infrastrukturo je potrebna specifična pozornost, saj prinaša svojstvena tveganja zaradi dejstva, da bi se lahko tehnologija za prepoznavanje obraza uporabljala neopazno in bi bila zlahka skrita[5].

2.2 Zelo raznovrstni nameni in vrste uporabe

16. Zunaj področja uporabe teh smernic in zunaj področja uporabe Direktive (EU) 2016/680 se lahko prepoznavanje obrazov uporablja za najrazličnejše cilje, tako za komercialno uporabo kot tudi za obravnavanje vprašanj javne varnosti ali kazenskega pregona. Možnosti uporabe so zelo raznovrstne: v osebnem razmerju med uporabnikom in storitvijo (dostop do aplikacije), za dostop do specifičnega mesta (fizično filtriranje) ali brez posebnih omejitev na javni površini (prepoznavanje obrazov v živo). Uporablja se lahko za vse vrste posameznikov, na katere se nanašajo osebni podatki: na stranke storitve, zaposlene, navadne opazovalce, iskane osebe ali osebe, vpletene v pravne ali upravne postopke, itd. Nekatere vrste uporabe so že običajne in razširjene, druge pa so za zdaj v poskusni fazi ali fazi špekulativnega preizkušanja. Čeprav v teh smernicah ne bodo obravnavane vse take uporabe in aplikacije, EOVP opozarja, da se lahko izvajajo le, če so skladne s pravnim okvirom, ki se uporablja, ter zlasti s Splošno uredbo o varstvu podatkov in ustrezno nacionalno zakonodajo[6]. Tudi v okviru Direktive (EU) 2016/680 se lahko poleg funkcij avtentikacije ali identifikacije podatki, ki se obdelujejo z uporabo tehnologije za prepoznavanje obraza, nadalje obdelujejo tudi za druge namene, na primer za kategorizacijo.

17. Natančneje, obseg možnih uporab bi se lahko upošteval glede na stopnjo nadzora, ki ga imajo ljudje nad svojimi osebnimi podatki, učinkovita sredstva, ki jih imajo za izvajanje takega nadzora, njihovo pravico do pobude za uvedbo in uporabo te tehnologije, posledice zanje (v primeru prepoznave ali neprepoznavne) in obseg izvedene obdelave. Prepoznavanje obraza na podlagi predloge, shranjene v osebni napravi (pametna kartica, pametni telefon itd.) v lasti zadevne osebe, ki se uporablja za avtentikacijo in strogo osebno uporabo prek namenskega vmesnika, ne prinaša enakih tveganj kot na primer uporaba za namene identifikacije v nenadzorovanem okolju brez dejavnega sodelovanja posameznikov, na katere se nanašajo osebni podatki, kadar se predloga obraza vsake osebe, ki vstopa na območje spremljanja, primerja s predlogami širokega preseka prebivalstva, shranjenimi v

[4] 10. člen Direktive (EU) 2016/680 (ali 9. člen Splošne uredbe o varstvu podatkov) se uporablja za sisteme, ki se uporabljajo za razvrščanje posameznikov na podlagi njihovih biometričnih podatkov v skupine glede na etnično pripadnost, politično ali spolno usmerjenost ali druge posebne vrste osebnih podatkov.

[5] Na primer pri kamerah, ki se nosijo na telesu in se v praksi uporabljajo čedalje pogosteje.

[6] Za dodatne usmeritve glej še Smernice Evropskega odbora za varstvo podatkov 3/2019 o obdelavi osebnih podatkov z video napravami, sprejete 29. januarja 2020.

podatkovni zbirki. Med tema skrajnostma so zelo raznovrstne možnosti uporabe in raznovrstna povezana vprašanja v zvezi z varstvom osebnih podatkov.

18. Da bi dodatno ponazoril kontekst, v katerem se trenutno razpravlja o tehnologijah za prepoznavanje obraza ali se te tehnologije izvajajo za avtentikacijo ali identifikacijo, EOVP meni, da je treba navesti številne primere. Primeri v nadaljevanju so zgolj opisni in se ne smejo šteti kot kakršna koli predhodna ocena njihove skladnosti s pravnim redom EU na področju varstva podatkov.

Primeri avtentikacije s prepoznavanjem obraza

19. Avtentikacija je lahko zasnovana tako, da imajo uporabniki popoln nadzor nad njo, na primer tako, da se omogoči dostop do storitev ali aplikacij izključno v domačem okolju. Tako jo lastniki pametnih telefonov pogosto uporabljajo za odklepanje svoje naprave namesto avtentikacije z geslom.

20. Avtentikacija s prepoznavanjem obraza se lahko uporablja tudi za preverjanje identitete osebe, ki želi izkoristiti javne ali zasebne storitve tretjih oseb. Taki postopki tako omogočajo način ustvarjanja digitalne identitete z uporabo mobilne aplikacije (pametni telefon, tablični računalnik itd.), ki se lahko nato uporabi za dostop do spletnih upravnih storitev.

21. Poleg tega je lahko cilj avtentikacije s prepoznavanjem obraza nadzor fizičnega dostopa do ene ali več vnaprej določenih lokacij, kot so vhodi v stavbe ali specifične točke prehoda. Ta funkcija se izvaja na primer pri nekaterih obdelavah za namene prehoda meje, pri čemer se obraz osebe na napravi na kontrolni točki primerja z obrazom, shranjenim v njenem osebnem dokumentu (potnem listu ali dovoljenju za prebivanje).

Primeri identifikacije s prepoznavanjem obraza

22. Identifikacija se lahko uporablja na številne, še bolj raznovrstne načine. Ti med drugim vključujejo v nadaljevanju navedene načine uporabe, ki so trenutno zaznani, se preizkušajo ali se načrtujejo v EU:

- iskanje identitete neidentificirane osebe (žrtve, osumljenca itd.) v podatkovni zbirki fotografij;
- spremljanje gibanja osebe v javnosti. Obraz te osebe se primerja z biometričnimi predlogami oseb, ki potujejo ali so potovale na nadzorovanem območju, na primer: če je nekje ostal kos prtljage ali je bilo storjeno kaznivo dejanje;
- rekonstrukcija potovanja osebe in njenih poznejših interakcij z drugimi osebami z zapoznelo primerjavo istih elementov, da bi na primer prepoznali osebe, s katerimi je bila v stiku;
- biometrična identifikacija iskanih oseb v javnosti na daljavo. Vse slike obrazov, zajete v živo s kamerami za videonadzor in varnost, se v realnem času navzkrižno preverijo s slikami v podatkovni zbirki varnostnih organov;
- avtomatizirano prepoznavanje oseb na sliki za identifikacijo, na primer njihovih odnosov v družbenem omrežju, na katerem je objavljena zadevna slika. Slika se primerja s predlogami vseh uporabnikov v zadevnem omrežju, ki so dali soglasje za to funkcijo, da se lahko izvede poimenska identifikacija oseb v teh razmerjih;
- dostop do storitev, pri čemer nekateri avtomati za dvig gotovine prepoznajo svoje stranke, tako da primerjajo sliko obraza, posneto s kamero, s slikami obraza v podatkovni zbirki, ki jo hrani banka;
- sledenje potniku na potovanju v določeni fazi potovanja. Predloga, izračunana v realnem času, vsake osebe, ki se prijavi pri vratih na določenih stopnjah potovanja (mesta za oddajo prtljage, vrata za vkrcanje itd.), se primerja s predlogami oseb, ki so bile predhodno registrirane v sistemu.

23. Poleg uporabe tehnologije za prepoznavanje obraza na področju kazenskega pregona sta zaradi zelo raznovrstnih zaznanih uporab nedvomno potrebna obsežna razprava in politični pristop, da se zagotovita doslednost in skladnost s pravnim redom EU na področju varstva podatkov.

2.3 Zanesljivost, natančnost in tveganja za posameznike, na katere se nanašajo osebni podatki

24. Tako kot vsaka tehnologija so tudi pri prepoznavanju obraza izzivi pri izvajanju, zlasti kar zadeva zanesljivost in učinkovitost v smislu avtentikacije ali identifikacije ter splošno vprašanje kakovosti in točnosti izvornih podatkov ter rezultatov obdelave s tehnologijo prepoznavanja obraza.

25. Tovrstni tehnološki izzivi prinašajo posebna tveganja za zadevne posameznike, na katere se nanašajo osebni podatki, ki so na področju kazenskega pregona še toliko pomembnejša ali resnejša, ob upoštevanju možnih pravnih ali drugih učinkov, ki na podoben način pomembno vplivajo na posameznike, na katere se nanašajo osebni podatki. V tem okviru se zdi koristno poudariti še, da naknadna uporaba tehnologije za prepoznavanje obraza sama po sebi ni varnejša, saj je mogoče posameznikom slediti v času in prostoru. Prav zato tudi naknadna uporaba prinaša specifična tveganja, ki jih je treba proučiti za vsak primer posebej[7].

26. Kot je Agencija EU za temeljne pravice poudarila v svojem poročilu iz leta 2019, je *določitev potrebne ravni točnosti programske opreme za prepoznavanje obraza zahtevna: možnih je veliko načinov vrednotenja in ocenjevanja točnosti, ki so odvisni tudi od naloge, namena in konteksta njene uporabe. Pri uporabi tehnologije na mestih, ki jih obišče več milijonov ljudi, kot so železniške postaje ali letališča, razmeroma majhen delež napak (na primer 0,01 %)*[8] *še vedno pomeni, da je več sto ljudi napačno označenih. Poleg tega je lahko pri nekaterih kategorijah ljudi verjetnost, da bo ujemanje napačno, večja kot pri drugih, kot je opisano v oddelku 3. Možni so različni načini za izračun in razlago stopenj napak, zato je potrebna previdnost. Poleg tega so v zvezi s točnostjo in napakami pomembna vprašanja, povezana s tem, kako zlahka je mogoče sistem prevarati, na primer z lažnimi slikami obrazov (tako imenovano slepljenje), zlasti za namene kazenskega pregona*.[9]

27. Glede tega je po mnenju EOVP pomembno opozoriti, da tehnologije za prepoznavanje obraza, ki se uporabljajo za namene avtentikacije ali identifikacije, ne zagotavljajo dokončnega rezultata, temveč se opirajo na verjetnost, da dva obraza ali sliki obrazov ustrezata isti osebi[10]. Ta rezultat se še poslabša, kadar je kakovost biometričnega vzorca, vnesenega v tehnologijo za prepoznavanje obraza, slaba. Dejavniki slabe kakovosti so lahko zamegljenost vhodnih slik, nizka ločljivost kamere, gibanje in slaba svetloba. Druga vidika, ki pomembno vplivata na rezultate, sta razširjenost in slepljenje, na primer kadar se storilci kaznivih dejanj poskušajo izogniti prehodu mimo kamer ali poskušajo prevarati tehnologijo za prepoznavanje obraza. V številnih študijah so poudarili še, da so lahko taki statistični rezultati algoritemske obdelave izpostavljeni tudi pristranskosti, ki je posledica zlasti kakovosti izvornih podatkov in podatkovnih zbirk za usposabljanje ali drugih dejavnikov, kot je izbira lokacije namestitve. Poleg tega je treba poudariti še vpliv tehnologije za prepoznavanje obraza na druge temeljne pravice, kot so spoštovanje zasebnega in družinskega življenja, svoboda izražanja in obveščanja, svoboda zbiranja in združevanja itd.

[7] Glej primere, navedene v Prilogi III.

[8] Ta stopnja točnosti izhaja iz citiranega poročila in izraža stopnjo, ki je veliko boljša od trenutne uspešnosti algoritmov v aplikacijah za prepoznavanje obraza.

[9] Facial recognition technology: fundamental rights considerations in the context of law enforcement (Tehnologija za prepoznavanje obraza: vidiki temeljnih pravic v okviru kazenskega pregona), Agencija EU za temeljne pravice, 21. november 2019.

[10] Ta verjetnost se imenuje ocena zaupanja.

28. Zato je ključno, da se zanesljivost in točnost tehnologije za prepoznavanje obraza upoštevata kot merili za ocenjevanje skladnosti s ključnimi načeli varstva podatkov v skladu s 4. členom Direktive (EU) 2016/680, zlasti kar zadeva poštenost in točnost.

29. EOVP poudarja, da so za visokokakovostne algoritme ključni visokokakovostni podatki, hkrati pa poudarja še, da morajo upravljavci podatkov v okviru svoje obveznosti glede odgovornosti redno in sistematično vrednotiti algoritemsko obdelavo, da bi zagotovili zlasti točnost, poštenost in zanesljivost rezultatov take obdelave osebnih podatkov. Osebni podatki, ki se uporabljajo za namene vrednotenja, usposabljanja in nadaljnjega razvoja sistemov za prepoznavanje obraza, se lahko obdelujejo le na podlagi zadostne pravne podlage in v skladu s skupnimi načeli varstva podatkov.

3 PRAVNI OKVIR, KI SE UPORABLJA

30. Uporaba tehnologij za prepoznavanje obraza je neločljivo povezana z obdelavo osebnih podatkov, vključno s posebnimi vrstami podatkov. Poleg tega ima neposreden ali posreden vpliv na številne temeljne pravice iz Listine EU o temeljnih pravicah. To je pomembno zlasti na področjih kazenskega pregona in kazenskega pravosodja. Zato bi bilo treba vsako uporabo tehnologij za prepoznavanje obraza izvajati ob strogem upoštevanju veljavnega pravnega okvira.

31. Naslednje informacije so namenjene premisleku pri ocenjevanju prihodnjih zakonodajnih in upravnih ukrepov ter izvajanju veljavne zakonodaje za vsak primer, ki vključuje tehnologijo za prepoznavanje obraza, posebej. Ustreznost posameznih zahtev se razlikuje glede na posebne okoliščine. Ker vseh prihodnjih okoliščin ni mogoče predvideti, se šteje, da so le v podporo in se ne upoštevajo kot izčrpen seznam.

3.1 Splošni pravni okvir – Listina EU o temeljnih pravicah in Evropska konvencija o človekovih pravicah (EKČP)

3.1.1 Upoštevnost Listine

32. Listina EU o temeljnih pravicah (v nadaljevanju: Listina) je naslovljena na institucije, organe, urade in agencije Unije ter na države članice, ko izvajajo pravo Unije.

33. Pri urejanju obdelave biometričnih podatkov za namene kazenskega pregona v skladu s prvim odstavkom 1. člena Direktive (EU) 2016/680 se neizogibno odpira vprašanje skladnosti s temeljnimi pravicami, zlasti spoštovanja zasebnega življenja in komunikacij iz 7. člena Listine ter pravice do varstva osebnih podatkov iz 8. člena Listine.

34. Zbiranje in analiza videoposnetkov fizičnih oseb, vključno z njihovimi obrazi, pomenita obdelavo osebnih podatkov. Pri tehnični obdelavi slike obdelava zajema tudi biometrične podatke. Tehnična obdelava podatkov, ki se nanašajo na obraz fizične osebe glede na čas in kraj, omogoča sklepanje v zvezi z zasebnim življenjem zadevnih oseb. Te sklepne ugotovitve se lahko nanašajo na rasno ali etnično poreklo, zdravje, veroizpoved, navade v vsakdanjem življenju, stalno ali začasno prebivališče, vsakodnevno ali drugo gibanje, dejavnosti, ki jih opravljajo, družbene odnose teh oseb in družbena okolja, ki jih obiskujejo. Velik obseg informacij, ki se lahko razkrijejo z uporabo tehnologije za prepoznavanje obraza, jasno kaže na možen vpliv na pravico do varstva osebnih podatkov iz 8. člena Listine in pravico do zasebnosti iz 7. člena Listine.

35. V takih okoliščinah ni izključeno, da bi zbiranje, analiza in nadaljnja obdelava zadevnih biometričnih podatkov (obraza) lahko vplivali na to, kako svobodni se ljudje počutijo pri ukrepanju, tudi če bi bilo ravnanje v celoti v duhu svobodne in odprte družbe. To bi lahko imelo resne posledice tudi za uresničevanje njihovih temeljnih pravic, kot so pravice do svobode misli, vesti in vere, do svobode izražanja ter do svobode zbiranja in združevanja iz 10., 11. oziroma 12. člena Listine. Taka obdelava vključuje še druga tveganja, kot je tveganje zlorabe osebnih podatkov, ki jih zberejo ustrezni organi, zaradi nezakonitega dostopa do osebnih podatkov in njihove uporabe, kršitve varnosti itd. Tveganja so pogosto odvisna od obdelave in njenih okoliščin, kot je tveganje nezakonitega dostopa policistov ali drugih nepooblaščenih oseb in njihove uporabe podatkov. Nekatera tveganja pa so preprosto neločljivo povezana z edinstveno naravo biometričnih podatkov. V nasprotju z naslovom ali telefonsko številko posameznik, na katerega se nanašajo osebni podatki, ne more spremeniti svojih edinstvenih značilnosti, kot sta obraz ali šarenica. V primeru nepooblaščenega dostopa do biometričnih podatkov ali nenamerne objave teh bi to povzročilo, da bi bila ogrožena uporaba teh podatkov kot gesel ali kriptografskih ključev ali pa bi se lahko uporabili za nadaljnje dejavnosti nepooblaščenega nadzora v škodo posameznika, na katerega se nanašajo osebni podatki.

3.1.2 Poseganje v pravice iz Listine

36. Obdelava biometričnih podatkov v vseh okoliščinah je že sama po sebi resno poseganje. To ni odvisno od rezultata, na primer pozitivnega ujemanja. Obdelava pomeni poseg tudi, če se biometrična predloga izbriše nemudoma po tem, ko se izkaže, da ni ujemanja s podatki iz policijske zbirke podatkov.

37. Poseganje v temeljne pravice posameznikov, na katere se nanašajo osebni podatki, lahko izhaja iz pravnega akta, katerega cilj je omejiti zadevno temeljno pravico ali ki učinkuje tako, da jo omejuje[11]. Lahko je tudi posledica dejanja javnega organa z enakim namenom ali učinkom ali celo zasebnega subjekta, ki v skladu s pravom lahko opravlja javne funkcije in izvaja javna pooblastila.

38. Zakonodajni ukrep, ki je pravna podlaga za obdelavo osebnih podatkov, neposredno posega v pravice, zagotovljene v 7. in 8. členu Listine[12].

39. Uporaba biometričnih podatkov in zlasti tehnologije za prepoznavanje obraza v številnih primerih vpliva tudi na pravico do človekovega dostojanstva, ki jo zagotavlja 1. člen Listine. Za spoštovanje človekovega dostojanstva je nujno, da se posamezniki ne obravnavajo zgolj kot predmeti. Tehnologija za prepoznavanje obraza pretvori eksistencialne in zelo osebne značilnosti, obrazne poteze, v strojno berljivo obliko, da jih uporabi kot osebno identifikacijsko tablico ali osebno izkaznico, s čimer obraz objektivizira.

40. Taka obdelava lahko posega tudi v druge temeljne pravice, kot so pravice iz 10., 11. in 12. člena Listine, če ustrezni videonadzor organov kazenskega pregona vzbuja zastraševalne učinke ali so ti učinki posledica tega nadzora.

41. Poleg tega je treba skrbno proučiti morebitna tveganja, ki jih povzroča uporaba tehnologij za prepoznavanje obraza pri kazenskem pregonu v zvezi s pravico do nepristranskega sodišča in domnevo nedolžnosti iz 47. oziroma 48. člena Listine. Rezultat uporabe tehnologije za prepoznavanje obraza, na primer ujemanje, lahko privede ne le do tega, da je oseba predmet nadaljnjega policijskega nadzora, temveč je lahko tudi odločilen dokaz v sodnem postopku. Pomanjkljivosti te tehnologije, kot so morebitna pristranskost, diskriminacija ali napačna identifikacija (lažno pozitiven), imajo lahko resne posledice tudi za kazenske postopke. Poleg tega je lahko pri presoji dokazov rezultat uporabe

[11] Sodišče Evropske unije, C-219/91 *Ter Voort*, RoC 1992 I-05485, točka 36f; Sodišče Evropske unije, C-200/96 *Metronome*, RoC 1998 I-1953, točka 28.

[12] Sodišče Evropske unije, C-594/12, točka 36; Sodišče Evropske unije, C-291/12, točka 23 in naslednje.

tehnologije za prepoznavanje obraza ugodnejši, tudi če obstajajo nasprotujoči si dokazi (pristranskost zaradi avtomatizacije).

3.1.3 Upravičenost poseganja

42. V skladu s prvim odstavkom 52. člena Listine mora biti kakršno koli omejevanje uresničevanja temeljnih pravic in svoboščin predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Evropska unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.

3.1.3.1 Predpisano z zakonodajo

43. Prvi odstavek 52. člena Listine določa zahtevo po specifični pravni podlagi. Ta pravna podlaga mora biti vsebinsko dovolj jasna, da se državljanom ustrezno pojasnijo pogoji in okoliščine, v katerih so organi pooblaščeni, da lahko uporabijo katere koli ukrepe za zbiranje podatkov in tajno opazovanje[13]. V njej morata biti z razumno jasnostjo navedena področje uporabe in način izvajanja ustrezne diskrecijske pravice, dodeljene javnim organom, s čimer se posameznikom zagotovi minimalna raven varstva, do katere so upravičeni v skladu z načelom pravne države v demokratični družbi[14]. Poleg tega zakonitost zahteva ustrezne zaščitne ukrepe, ki zagotavljajo zlasti spoštovanje posameznikove pravice iz 8. člena Listine. Ta načela se uporabljajo tudi za obdelavo osebnih podatkov za namene ocenjevanja, usposabljanja in nadaljnjega razvoja sistemov za prepoznavanje obraza.

44. Glede na to, da biometrični podatki, ki se obdelujejo za namene edinstvene identifikacije posameznika, spadajo med posebne vrste podatkov iz 10. člena Direktive (EU) 2016/680, bi bilo treba za različne vrste uporabe tehnologije za prepoznavanje obraza v večini primerov sprejeti poseben zakon, v katerem bi bili natančno opredeljeni uporaba in pogoji zanjo. To zajema zlasti vrste kaznivih dejanj in, kadar je ustrezno, ustrezen prag resnosti teh kaznivih dejanj, da se med drugim učinkovito izključijo manjša kazniva dejanja[15].

3.1.3.2 Bistvo temeljnih pravic do zasebnosti in do varstva osebnih podatkov iz 7. oziroma 8. člena Listine

45. Ob omejitvah temeljnih pravic, ki so neposredno povezane s posameznim položajem, se mora še vedno zagotavljati bistvo posamezne pravice, ki jo je treba spoštovati. Bistvo se nanaša na jedro zadevne temeljne pravice[16]. Spoštovati je treba tudi človekovo dostojanstvo, kadar je uresničevanje pravice omejeno[17].

46. Znaki morebitne kršitve nedotakljivega jedra so:

- določba, ki določa omejitve ne glede na posameznikovo ravnanje ali izjemne okoliščine[18];
- uporaba sodnih postopkov ni mogoča ali je ovirana[19];
- pred strogo omejitvijo se ne upoštevajo okoliščine zadevnega posameznika[20];

[13] ESČP, *Shimovolos proti Rusiji*, § 68; *Vukota-Bojić proti Švici*.
[14] ESČP, *Piechowicz proti Poljski*, § 212.
[15] Glej na primer sodbi Sodišča Evropske unije v zadevah C-817/19 *Ligue des droits humains*, točka 151, in C-207/16 *Ministerio Fiscal*, točka 56.
[16] Sodišče Evropske unije, C-279/09, RoC 2010 I-13849, točka 60.
[17] Pojasnila k Listini o temeljnih pravicah, Naslov I, Pojasnilo k členu 1, UL C 303, 14. 12. 2007, str. 17–35.
[18] Sodišče Evropske unije, C-601/15, točka 52.
[19] Sodišče Evropske unije, C-400/10, RoC 2010 I-08965, točka 55.
[20] Sodišče Evropske unije, C-408/03, RoC 2006 I-02647, točka 68.

- ob upoštevanju pravic iz 7. in 8. člena Listine: poleg obsežne zbirke komunikacijskih metapodatkov bi se lahko ob seznanjenosti z vsebino elektronske komunikacije kršilo bistvo teh pravic[21];
- ob upoštevanju pravic iz 7., 8. in 11. člena Listine: zakonodaja, v skladu s katero se zahteva, da ponudniki dostopa do javnih spletnih komunikacijskih storitev in ponudniki storitev gostovanja na splošno in brez razlikovanja hranijo med drugim osebne podatke, ki se nanašajo na navedene storitve[22];
- v zvezi s pravicami iz 8. člena Listine: tudi pomanjkanje temeljnih načel varstva podatkov in varnosti podatkov bi lahko kršilo bistvo pravice[23].

3.1.3.3 Zakoniti cilj

47. Kot je že pojasnjeno v točki 3.1.3, morajo omejitve pri uresničevanju temeljnih pravic dejansko ustrezati ciljem splošnega interesa, ki jih priznava Evropska unija, ali mora biti izpolnjena potreba po zaščiti pravic in svoboščin drugih.

48. Unija priznava cilje, navedene v 3. členu Pogodbe o Evropski uniji, in druge interese, ki so zaščiteni s posebnimi določbami Pogodb[24], med drugim oblikovanje območja svobode, varnosti in pravice ter preprečevanje kriminalitete in boj proti njej. Unija bi morala v svojih odnosih s preostalim svetom prispevati k miru in varnosti ter varstvu človekovih pravic.

49. Potreba po varstvu pravic in svoboščin drugih se nanaša na pravice oseb, ki so zaščitene s pravom Evropske unije ali njenih držav članic. Ocena mora biti izvedena, da se uskladijo zahteve glede varstva zadevnih pravic in da se vzpostavi pravično ravnotežje med njimi[25].

3.1.3.4 Preizkus nujnosti in sorazmernosti

50. Kadar gre za posege v temeljne pravice, se lahko izkaže, da je obseg diskrecijske pravice nacionalnega zakonodajalca in zakonodajalcev Unije omejen. To je odvisno od številnih dejavnikov, vključno z zadevnim področjem, naravo zadevne pravice, zagotovljene z Listino, naravo in resnostjo posega ter ciljem, ki se ga želi doseči s posegom[26]. Zakonodajni ukrepi morajo biti ustrezni za doseganje legitimnih ciljev v skladu z zadevno zakonodajo. Poleg tega ukrep ne sme preseči omejitev tistega, kar je ustrezno in potrebno, da se dosežejo navedeni cilji[27]. Cilj v splošnem interesu, tudi če je temeljni, sam po sebi ne more upravičiti omejevanja temeljne pravice[28].

51. V skladu z ustaljeno sodno prakso Sodišča Evropske unije se smejo odstopanja in omejitve v zvezi z varstvom osebnih podatkov uporabljati le, če je to nujno potrebno[29]. To pomeni tudi, da za dosego cilja niso na voljo manj vsiljiva sredstva. Treba je skrbno opredeliti in oceniti morebitne alternative, kot so – odvisno od zadevnega namena – dodatno osebje, pogostejše policijsko ukrepanje ali dodatna ulična

---

[21] Sodišče Evropske unije, 203/15 *Tele2 Sverige*, točka 101 s sklicevanjem na Sodišče Evropske unije, C-293/12 in C-594/12, točka 39.
[22] Sodišče Evropske unije, C-512/18 *La Quadrature du Net*, točka 209 in naslednje.
[23] Sodišče Evropske unije, C-594/12, točka 40.
[24] Pojasnila k Listini o temeljnih pravicah, Naslov I, Pojasnilo k členu 52, UL C 303, 14. 12. 2007, str. 17–35.
[25] Jarass, GrCh, 3. izdaja, 2016, Listina EU o temeljnih pravicah, člen 52, str. 31 in 32.
[26] Sodišče Evropske unije, C-594/12, točka 47 z naslednjimi viri: glej po analogiji v zvezi z 8. členom EKČP, sodba ESČP v zadevi *S. in Marper proti Združenemu kraljestvu* (veliki senat), št. 30562/04 in 30566/04, § 102, ECHR 2008-V.
[27] Sodišče Evropske unije, C-594/12, točka 46 z naslednjimi viri: zadeva C-343/09 *Afton Chemical*, EU:C:2010:419, točka 45; *Volker und Markus Schecke and Eifert*, EU:C:2010:662, točka 74; zadevi C-581/10 in C-629/10 *Nelson in drugi*, EU:C:2012:657, točka 71; zadeva C-283/11 *Sky Österreich*, EU:C:2013:28, točka 50; in zadeva C-101/12 *Schaible*, EU:C:2013:661, točka 29.
[28] Sodišče Evropske unije, C-594/12, točka 51.
[29] Sodišče Evropske unije, C-594/12, točka 52, z naslednjim virom: zadeva C-473/12 *IPI*, EU:C:2013:715, točka 39 in navedena sodna praksa.

razsvetljava. Zakonodajni ukrepi bi morali razlikovati med osebami in biti usmerjeni na osebe, za katere veljajo, glede na cilj, na primer za boj proti hudemu kaznivemu dejanju. Če na splošno zajemajo vse osebe, tj. brez takega razlikovanja, omejitve ali izjeme, se okrepijo[30]. To se zgodi tudi, kadar obdelava podatkov zajema pomemben del prebivalstva[31].

52. Varstvo osebnih podatkov, ki izhaja iz izrecne obveznosti iz prvega odstavka 8. člena Listine, je še posebej pomembno za pravico do spoštovanja zasebnega življenja iz 7. člena Listine[32]. V zakonodaji je treba opredeliti jasna in natančna pravila, ki urejajo področje uporabe in uporabo zadevnega ukrepa, ter uvesti zaščitne ukrepe, tako da imajo osebe, katerih podatki so bili obdelani, zadostna jamstva za učinkovito varstvo svojih osebnih podatkov pred tveganjem zlorabe in pred katerim koli nezakonitim dostopom ali uporabo navedenih podatkov[33]. Potreba po takih zaščitnih ukrepih je še toliko večja, kadar se osebni podatki obdelujejo avtomatizirano in kadar obstaja velika nevarnost nezakonitega dostopa do podatkov[34]. Poleg tega lahko k zaščitnim ukrepom pripomore notranja ali zunanja, na primer sodna, odobritev uporabe tehnologije za prepoznavanje obraza, ki se lahko izkaže za potrebno v nekaterih primerih resnih posegov[35].

53. Nekatera pravila je treba prilagoditi specifičnim razmeram, na primer količini obdelanih podatkov, naravi podatkov[36] in tveganju nezakonitega dostopa do podatkov. Zato so potrebna pravila, s katerimi bi se zlasti jasno in strogo uredila varstvo in varnost zadevnih podatkov, da se zagotovita njihova popolna celovitost in zaupnost[37].

54. V zvezi z odnosom med upravljavcem in obdelovalcem ne bi smelo biti dovoljeno, da bi obdelovalci pri določanju ravni varnosti, ki jo uporabljajo za osebne podatke, upoštevali le gospodarske vidike; to bi lahko ogrozilo zadostno raven varstva[38].

55. V pravnem aktu morajo biti opredeljeni vsebinski in postopkovni pogoji ter objektivna merila, na podlagi katerih se določijo omejitve dostopa pristojnih organov do podatkov in njihove poznejše uporabe. Za namene preprečevanja, odkrivanja ali pregona kaznivih dejanj bi bilo treba zadevna kazniva dejanja šteti za dovolj resna, da bi se upravičila obseg in resnost teh posegov v temeljne pravice, zagotovljene na primer v 7. in 8. členu Listine[39].

56. Podatke je treba obdelovati na način, ki zagotavlja uporabo in učinek pravil EU o varstvu podatkov, zlasti tistih iz 8. člena Listine, ki določa, da izpolnjevanje zahtev o varstvu in varnosti nadzira neodvisni organ. V takem primeru je lahko pomembno geografsko območje, na katerem poteka obdelava[40].

---

[30] Sodišče Evropske unije, C-594/12, točka 57.
[31] Sodišče Evropske unije, C-594/12, točka 56.
[32] Sodišče Evropske unije, C-594/12, točka 53.
[33] Sodišče Evropske unije, C-594/12, točka 54, z naslednjimi viri: glej po analogiji, kar zadeva 8. člen EKČP, sodbe ESČP v zadevah *Liberty in drugi proti Združenemu kraljestvu*, 1. julij 2008, št. 58243/00, § 62 in 63; *Rotaru proti Romuniji*, § 57 do 59, ter *S. in Marper proti Združenemu kraljestvu*, § 99.
[34] Sodišče Evropske unije, C-594/12, točka 55, z naslednjima viroma: glej po analogiji, kar zadeva 8. člen EKČP, *S. in Marper proti Združenemu kraljestvu*, § 103, in *M. K. proti Franciji*, 18. april 2013, št. 19522/09, § 35.
[35] ESČP, *Szabó in Vissy proti Madžarski*, § 73–77.
[36] Glej tudi strožje zahteve za tehnične in organizacijske ukrepe pri obdelavi posebnih vrst podatkov, prvi odstavek 29. člena Direktive (EU) 2016/680.
[37] Sodišče Evropske unije, C-594/12, točka 66.
[38] Sodišče Evropske unije, C-594/12, točka 67.
[39] Sodišče Evropske unije, C-594/12, točki 60 in 61.
[40] Sodišče Evropske unije, C-594/12, točka 68.

57. V zvezi z različnimi koraki obdelave osebnih podatkov bi bilo treba razlikovati med vrstami podatkov na podlagi njihove možne uporabnosti za namene postavljenega cilja ali glede na zadevne osebe[41]. Opredelitev pogojev obdelave, na primer opredelitev obdobja hrambe, mora temeljiti na objektivnih merilih, s čimer se zagotovi, da je poseganje omejeno na to, kar je nujno potrebno[42].

58. Na podlagi posamezne okoliščine je treba pri presoji nujnosti in sorazmernosti opredeliti in upoštevati vse posledice, ki spadajo na področje uporabe drugih temeljnih pravic, kot so človekovo dostojanstvo iz 1. člena Listine, svoboda misli, vesti in vere iz 10. člena Listine, svoboda izražanja iz 11. člena Listine ter svoboda zbiranja in združevanja iz 12. člena Listine.

59. Poleg tega je treba upoštevati, da je zelo verjetno, da lahko, če se podatki sistematično obdelujejo brez vednosti posameznikov, na katere se nanašajo osebni podatki, to vzbuja splošni občutek stalnega nadzora[43]. To lahko ustvari zastraševalne učinke v zvezi z nekaterimi ali vsemi zadevnimi temeljnimi pravicami.

60. Da bi olajšali in operacionalizirali presojo nujnosti in sorazmernosti zakonodajnih ukrepov v zvezi s prepoznavanjem obraza na področju kazenskega pregona, bi lahko nacionalni zakonodajalci in zakonodajalca Unije uporabili praktična orodja, ki so na voljo in ki so zasnovana posebej za to nalogo. Uporabiti bi bilo mogoče zlasti zbirko orodij za nujnost in sorazmernost[44], ki jo je pripravil Evropski nadzornik za varstvo podatkov.

3.1.3.5 Tretji odstavek 52. člena in 53. člen Listine (raven varstva, tudi v primerjavi z EKČP)

61. V skladu s tretjim odstavkom 52. člena in 53. členom Listine morata biti vsebina in obseg pravic iz Listine, ki ustrezajo pravicam, zagotovljenim z EKČP, enaka kot vsebina in obseg pravic, ki jih določa EKČP. Zlasti za 7. člen Listine je mogoče v EKČP najti ustreznico, za 8. člen Listine pa to ne velja[45]. Tretji odstavek 52. člena Listine ne preprečuje širšega varstva po pravu Unije. Glede na to, da EKČP ni pravni instrument, ki je bil formalno vključen v pravo Unije, je treba zakonodajo Unije sprejemati ob upoštevanju temeljnih pravic iz Listine[46].

62. V skladu z 8. členom EKČP se javna oblast ne sme vmešavati v izvrševanje te pravice do spoštovanja zasebnega in družinskega življenja, razen če je to določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato, da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

63. V EKČP so navedeni tudi standardi v zvezi s tem, kako se omejitve lahko izvajajo. Ena od temeljnih zahtev, poleg načela pravne države, je predvidljivost. Da bi bila izpolnjena zahteva po predvidljivosti, mora biti pravo vsebinsko dovolj jasno, da se posameznikom ustrezno opišejo okoliščine in pogoji, v

[41] Sodišče Evropske unije, C-594/12, točka 63.
[42] Sodišče Evropske unije, C-594/12, točka 64.
[43] Sodišče Evropske unije, C-594/12, točka 37.
[44] Evropski nadzornik za varstvo podatkov: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (Ocenjevanje potrebnosti ukrepov, ki omejujejo temeljno pravico do varstva osebnih podatkov: zbirka orodij) (11. april 2017); Evropski nadzornik za varstvo podatkov: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (Smernice Evropskega nadzornika za varstvo podatkov za presojo sorazmernosti ukrepov, ki omejujejo temeljni pravici do zasebnosti in do varstva osebnih podatkov) (19. december 2019).
[45] Sodišče Evropske unije, C-203/15 *Tele2 Sverige*, točka 129.
[46] Sodišče Evropske unije, C-311/18, točka 99.

katerih so organi pooblaščeni za uporabo takih ukrepov[47]. To zahtevo priznavata Sodišče Evropske unije in zakonodaja EU o varstvu podatkov (prim. oddelek 3.2.1.1).

64. Pri podrobnejši opredelitvi pravic iz 8. člena EKČP je treba v celoti spoštovati tudi določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[48]. Kljub temu je treba upoštevati, da so te določbe le minimalni standard glede na veljavno zakonodajo Unije.

3.2 Specifični pravni okvir: Direktiva (EU) 2016/680

65. Zadevni okvir v zvezi z uporabo tehnologije za prepoznavanje obraza je zagotovljen v Direktivi (EU) 2016/680. Prvič, v trinajstem odstavku 3. člena Direktive (EU) 2016/680 je opredeljen izraz „biometrični podatki“[49]. Za podrobnosti prim. oddelek 2.1 zgoraj. Drugič, v drugem odstavku 8. člena je pojasnjeno, da mora biti vsaka obdelava, da bi bila zakonita, poleg tega, da je potrebna za namene iz prvega odstavka 1. člena Direktive (EU) 2016/680, urejena v nacionalnem pravu, ki določa vsaj cilje obdelave, kateri osebni podatki se obdelajo in namene obdelave. Drugi določbi posebnega pomena v zvezi z biometričnimi podatki sta 10. in 11. člen Direktive (EU) 2016/680. Člen 10 je treba razlagati v povezavi z 8. členom Direktive (EU) 2016/680[50]. Vedno bi bilo treba upoštevati načela za obdelavo osebnih podatkov, kot so določena v 4. členu Direktive (EU) 2016/680, in v skladu z njimi opraviti vsako presojo morebitne obdelave biometričnih podatkov s tehnologijo za prepoznavanje obraza.

3.2.1 Obdelava posebnih vrst podatkov za namene kazenskega pregona

66. V skladu z 10. členom Direktive (EU) 2016/680 je obdelava posebnih vrst podatkov, kot so biometrični podatki, dovoljena le, če je nujno potrebna in če je zagotovljena ustrezna zaščita pravic in svoboščin posameznika, na katerega se podatki nanašajo. Poleg tega je obdelava dovoljena le, če to dovoljuje pravo Unije ali države članice, če je to potrebno zaradi zaščite življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugega posameznika ali če je taka obdelava povezana s podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi. Ta splošna določba poudarja občutljivost obdelave posebnih vrst podatkov.

3.2.1.1 Dovoljeno v skladu s pravom Unije ali pravom države članice

67. V zvezi s potrebno vrsto zakonodajnega ukrepa je v uvodni izjavi 33 Direktive (EU) 2016/680 navedeno: „Kadar se ta direktiva sklicuje na pravo države članice, pravno podlago ali zakonodajni ukrep, to, brez poseganja v ustavne zahteve zadevne države članice, ne pomeni nujno, da mora zakonodajni akt sprejeti parlament.“[51]

68. V skladu s prvim odstavkom 52. člena Listine mora biti kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava Listina, predpisano z zakonom. To izraža besedilo „določeno z zakonom“ iz

[47] Evropsko sodišče za človekove pravice, sodba v zadevi *Copland proti Združenemu kraljestvu*, 3. april 2007, pritožba št. 62617/00, točka 46.
[48] Zbirka pogodb Sveta Evrope, št. 108.
[49] Trinajsti odstavek 3. člena Direktive (EU) 2016/680: izraz „biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so slike obraza ali daktiloskopski podatki.
[50] Delovna skupina iz člena 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (Mnenje o nekaterih ključnih vprašanjih glede direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj) (Direktiva (EU) 2016/680), str. 7.
[51] Vrsta obravnavanih zakonodajnih ukrepov mora biti v skladu s pravom Unije ali nacionalnim pravom. Glede na stopnjo poseganja omejitve se lahko na nacionalni ravni zahteva poseben zakonodajni ukrep, pri čemer se upošteva raven norme.

drugega odstavka 8. člena EKČP, ki ne pomeni le spoštovanja prava, ki se uporablja, ampak se nanaša tudi na kakovost tega prava, ne da bi to vplivalo na naravo akta, ki mora biti združljivo s pravno državo.

69. V uvodni izjavi 33 Direktive (EU) 2016/680 je navedeno še: „Takšno pravo države članice, pravna podlaga ali zakonodajni ukrep pa bi morali biti za osebe, na katere se nanašajo, jasni in natančni, njihova uporaba pa predvidljiva, v skladu s sodno prakso Sodišča in Evropskega sodišča za človekove pravice. Pravo države članice, ki ureja obdelavo osebnih podatkov v okviru področja uporabe te direktive, bi moralo določiti vsaj cilje, osebne podatke, ki se obdelujejo, namene obdelave ter postopke za ohranjanje celovitosti in zaupnosti osebnih podatkov ter postopke za njihovo uničenje.“

70. Nacionalno pravo mora biti vsebinsko dovolj jasno, da se posameznikom, na katere se nanašajo osebni podatki, ustrezno pojasnijo okoliščine in pogoji, v katerih so upravljavci pooblaščeni, da lahko uporabijo take ukrepe. To vključuje morebitne predpogoje za obdelavo, kot so posebne vrste dokazov, in potrebo po sodni ali notranji odobritvi. Zadevna zakonodaja je lahko tehnološko nevtralna, če so posebna tveganja in značilnosti obdelave osebnih podatkov v sistemih za prepoznavanje obraza zadostno obravnavani. V skladu z Direktivo (EU) 2016/680 ter sodno prakso Sodišča Evropske unije in Evropskega sodišča za človekove pravice (ESČP) je dejansko bistveno, da so zakonodajni ukrepi, katerih cilj je zagotoviti pravno podlago za ukrep prepoznavanja obraza, predvidljivi za posameznike, na katere se nanašajo osebni podatki.

71. Na zakonodajni ukrep se ni mogoče sklicevati kot na zakon, ki dovoljuje obdelavo biometričnih podatkov z uporabo tehnologije za prepoznavanje obraza za namene kazenskega pregona, če gre zgolj za prenos splošne določbe iz 10. člena Direktive (EU) 2016/680.

72. Poleg biometričnih podatkov 10. člen Direktive (EU) 2016/680 ureja obdelavo drugih posebnih vrst podatkov, kot so spolna usmerjenost, politična stališča in veroizpoved, in tako zajema zelo raznovrstno obdelavo. Poleg tega taka določba ne bi vsebovala specifičnih zahtev, ki bi določale okoliščine in pogoje, v katerih bi bili organi kazenskega pregona pooblaščeni, da lahko uporabijo tehnologijo za prepoznavanje obraza. Zaradi sklicevanja na druge vrste podatkov in izrecne potrebe po posebnih zaščitnih ukrepih brez nadaljnjih specifikacij se na nacionalno določbo, s katero je bil v nacionalno zakonodajo prenesen 10. člen Direktive (EU) 2016/680 – s podobno splošnim in abstraktnim besedilom –, ni mogoče sklicevati kot na pravno podlago za obdelavo biometričnih podatkov, kar vključuje prepoznavanje obraza, saj bi bila premalo natančna in predvidljiva. Preden zakonodajalec ustvari novo pravno podlago za katero koli obliko obdelave biometričnih podatkov z uporabo prepoznavanja obrazov, se je treba v skladu z drugim odstavkom 28. člena ali točko c prvega odstavka 46. člena Direktive (EU) 2016/680 posvetovati z nacionalnim nadzornim organom za varstvo podatkov.

3.2.1.2 Nujno potrebno

73. Obdelava se lahko šteje za nujno potrebno le, če so poseg v varstvo osebnih podatkov in njegove omejitve omejeni na to, kar je izrecno potrebno[52]. Vključitev izraza „strogo“ pomeni, da je zakonodajalec nameraval obdelavo posebnih vrst podatkov dovoliti le pod pogoji, ki so še strožji od pogojev za nujnost (glej oddelek 3.1.3.4 zgoraj). To zahtevo je treba razlagati kot nujno potrebno. Z njo je diskrecijska pravica, ki jo ima organ kazenskega pregona pri preizkusu nujnosti, omejena na absolutni minimum. V skladu z ustaljeno sodno prakso Sodišča Evropske unije je pogoj stroge nujnosti tesno

[52] Ustaljena sodna praksa o temeljni pravici do spoštovanja zasebnega življenja, glej Sodišče Evropske unije, zadeva C-73/07 *Satakunnan Markkinapörssi in Satamedia*, točka 56; Sodišče Evropske unije, zadevi C-92/09 in C-93/09 *Schecke in Eifert*, točka 77; Sodišče Evropske unije, zadeva C-594/12 *Digitalne pravice* ,točka 52; Sodišče Evropske unije, zadeva C-362/14 *Schrems*, točka 92.

povezan tudi z zahtevo po objektivnih merilih za opredelitev okoliščin in pogojev, v katerih se lahko obdelava izvaja, s čimer je izključena vsakršna splošna ali sistematična obdelava[53].

3.2.1.3 Očitno javno objavljeno

74. Pri presoji, ali se obdelava nanaša na podatke, ki jih posameznik, na katerega se nanašajo osebni podatki, sam objavi, je treba opozoriti, da se fotografija kot taka sistematično ne šteje za biometrični podatek[54]. Zato dejstvo, da je posameznik, na katerega se nanašajo osebni podatki, sam objavil fotografijo, ne pomeni, da se povezani biometrični podatki, ki jih je mogoče s specifičnimi tehničnimi sredstvi pridobiti iz fotografije, štejejo za javne.

75. Kar zadeva osebne podatke na splošno, da bi se štelo, da je biometrične podatke sam objavil prav posameznik, na katerega se nanašajo osebni podatki, mora ta posameznik namenoma zagotoviti, da je biometrična predloga (ne le slika obraza) prosto dostopna in javna prek prosto dostopnega vira. Če biometrične podatke razkrije tretja oseba, ni mogoče šteti, da je posameznik, na katerega se nanašajo osebni podatki, podatke sam objavil.

76. Poleg tega razlaga vedenja posameznika, na katerega se nanašajo osebni podatki, ne zadošča za ugotovitev, da so bili biometrični podatki javno objavljeni. Na primer: v primeru družbenih omrežij ali spletnih platform EOVP meni, da dejstvo, da posameznik, na katerega se nanašajo osebni podatki, ni vključil ali določil specifičnih nastavitev zasebnosti, ne zadošča za ugotovitev, da je ta posameznik, na katerega se nanašajo osebni podatki, objavil svoje osebne podatke ter da se lahko ti podatki (na primer fotografije) obdelujejo v biometričnih predlogah in se uporabljajo za namene identifikacije brez privolitve posameznika, na katerega se nanašajo osebni podatki. Na splošno, privzete nastavitve storitve, na primer da so predloge javno dostopne, ali to, da izbira ni mogoča, na primer predloge se objavijo, uporabnik pa te nastavitve ne more spremeniti, se nikakor ne bi smele razlagati kot javno objavljeni podatki.

3.2.2 Avtomatizirano sprejemanje posameznih odločitev, vključno z oblikovanjem profilov

77. Prvi odstavek 11. člena Direktive (EU) 2016/680 določa, da morajo države članice na splošno prepovedati sprejemanje odločitev izključno na podlagi avtomatizirane obdelave, vključno z oblikovanjem profilov, ki ima negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ga zelo prizadene. Kot izjema od te splošne prepovedi je taka obdelava mogoča le, če je če to dovoljuje pravo Unije ali države članice, ki se uporablja za upravljavca in ki zagotavlja ustrezno zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, vsaj pravice do osebnega posredovanja s strani upravljavca. Uporablja se lahko samo omejeno. Ta prag velja za običajne (tj. ne posebne) vrste osebnih podatkov. Za izjemo iz drugega odstavka 11. člena Direktive (EU) 2016/680 veljata še višji prag in bolj omejevalna uporaba. Znova je poudarjeno, da odločitve iz prvega odstavka ne temeljijo na posebnih vrstah osebnih podatkov, tj. zlasti na biometričnih podatkih za namene edinstvene identifikacije fizične osebe. Izjema se lahko predvidi le, če so vzpostavljeni ustrezni ukrepi za zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, ter zakonitih interesov zadevne fizične osebe. To izjemo je treba razlagati poleg 10. člena Direktive (EU) 2016/680 in ob upoštevanju tega člena.

---

[53] Sodišče Evropske unije, zadeva C-623/17, točka 78.

[54] Prim. uvodno izjavo 51 Splošne uredbe o varstvu podatkov: „Obdelava fotografij se ne bi smela sistematično šteti za obdelavo posebnih vrst osebnih podatkov, saj spadajo v opredelitev biometričnih podatkov le, kadar so obdelane s posebnimi tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika.“

78. Odvisno od sistema za prepoznavanje obraza tudi osebno posredovanje pri presoji rezultatov tehnologije za prepoznavanje obraza samo po sebi ni nujno zadostno jamstvo, da se spoštujejo pravice posameznikov, zlasti pravice do varstva osebnih podatkov, če se upoštevajo možne pristranskosti in napake, ki so lahko posledica obdelave. Poleg tega se osebno posredovanje lahko šteje za zaščitni ukrep le, če lahko oseba, ki posreduje, med osebnim posredovanjem kritično presoja rezultate tehnologije za prepoznavanje obraza. Ključno je, da se osebi omogoči, da razume sistem za prepoznavanje obraza in njegove omejitve, ter da ustrezno razlaga njegove rezultate. Ob tem je treba vzpostaviti delovno mesto in organizacijo, ki bo preprečevala učinke pristranskosti zaradi avtomatizacije in se izogibala spodbujanju nekritičnega sprejemanja rezultatov, na primer zaradi časovnega pritiska, obremenjujočih postopkov, morebitnih škodljivih učinkov na poklicni poti itd.

79. V skladu s tretjim odstavkom 11. člena Direktive (EU) 2016/680 in pravom Unije je prepovedano oblikovanje profilov, katerega posledica je diskriminacijo posameznikov na podlagi posebnih vrst osebnih podatkov, kot so biometrični podatki. V skladu s četrtim odstavkom 3. člena Direktive (EU) 2016/680 izraz „oblikovanje profilov“ pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika. Pri presoji, ali so predvideni ustrezni ukrepi za zaščito pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, ter zakonitih interesov fizične osebe, je treba upoštevati, da lahko uporaba tehnologije za prepoznavanje obraza privede do oblikovanja profilov, odvisno od načina in namena uporabe te tehnologije. V vsakem primeru je v skladu s pravom Unije in tretjim odstavkom 11. člena Direktive (EU) 2016/680 prepovedano oblikovanje profilov, katerega posledica je diskriminacija posameznikov na podlagi posebnih vrst osebnih podatkov.

3.2.3 Kategorije posameznikov, na katere se nanašajo osebni podatki

80. Člen 6 Direktive (EU) 2016/680 obravnava potrebo po razlikovanju med različnimi kategorijami posameznikov, na katere se nanašajo osebni podatki. To razlikovanje je treba upoštevati, kadar je to ustrezno in v največji možni meri. Pokazati mora učinek na način, kako se podatki obdelujejo. Iz primerov iz 6. člena Direktive (EU) 2016/680 je mogoče sklepati, da mora obdelava osebnih podatkov praviloma izpolnjevati merili nujnosti in sorazmernosti tudi v zvezi s kategorijo posameznikov, na katere se nanašajo osebni podatki[55]. Poleg tega je mogoče sklepati, da v zvezi s posamezniki, na katere se nanašajo osebni podatki in za katere ni dokazov, na podlagi katerih bi bilo mogoče sklepati, da bi njihovo ravnanje lahko bilo povezano, bodisi posredno bodisi oddaljeno, z legitimnim ciljem v skladu z Direktivo (EU) 2016/680, poseg najverjetneje ni upravičen[56]. Če se razlikovanje iz 6. člena Direktive (EU) 2016/680 ne izvaja ali ni mogoče, je treba izjemo od pravila iz 6. člena Direktive (EU) 2016/680 strogo upoštevati pri presoji nujnosti in sorazmernosti posega. Razlikovanje med kategorijami posameznikov, na katere se nanašajo osebni podatki, se zdi bistvena zahteva pri obdelavi osebnih podatkov, ki vključuje prepoznavanje obrazov, tudi glede na morebitne lažno pozitivne ali lažno negativne zadetke, ki imajo lahko pomembne posledice za posameznike, na katere se nanašajo osebni podatki, in med potekom preiskave.

81. Kot je bilo že navedeno, je treba pri izvajanju prava Unije spoštovati določbe Listine Evropske unije o temeljnih pravicah, prim. 52. člen Listine. Okvir in merila, ki jih določa Direktiva (EU) 2016/680, je treba torej razlagati ob upoštevanju Listine. Temu ukrepu morajo slediti tudi pravni akti EU in njenih držav članic in morajo zagotavljati polni učinek Listine.

[55] Prim. tudi Sodišče Evropske unije, C-594/12, točke 56 do 59.
[56] Prim. tudi Sodišče Evropske unije, C-594/12, točka 58.

3.2.4 Pravice posameznika, na katerega se nanašajo osebni podatki

82. EOVP je že pripravil smernice o pravicah posameznikov, na katere se nanašajo osebni podatki, v skladu s Splošno uredbo o varstvu podatkov, in to z različnih vidikov[57]. Direktiva (EU) 2016/680 določa podobne pravice posameznikov, na katere se nanašajo osebni podatki, splošne smernice v zvezi s tem pa so bile navedene v mnenju Delovne skupine iz člena 29, ki ga je EOVP potrdil[58]. Direktiva (EU) 2016/680 v nekaterih okoliščinah omogoča nekatere omejitve teh pravic. Parametri za take omejitve bodo podrobneje opredeljeni v oddelku 3.2.4.6 Legitimne omejitve pravic posameznika, na katerega se nanašajo osebni podatki.

83. Čeprav vse pravice posameznikov, na katere se nanašajo osebni podatki, kot so navedene v III. poglavju Direktive (EU) 2016/680, seveda veljajo tudi za obdelavo osebnih podatkov s tehnologijo za prepoznavanja obraza, se bo naslednje poglavje osredotočilo na nekatere pravice in vidike, za katere bi lahko bilo še posebej koristno, da se zagotovijo smernice. Poleg tega sta to poglavje in njegova analiza odvisna od tega, ali zadevna obdelava s tehnologijo za prepoznavanje obraza izpolnjuje pravne zahteve, opisane v prejšnjem poglavju.

84. Glede na naravo obdelave osebnih podatkov s tehnologijo za prepoznavanje obraza (obdelava posebnih vrst osebnih podatkov pogosto brez vsakršne očitne vključitve posameznika, na katerega se nanašajo osebni podatki) mora upravljavec skrbno proučiti, kako (oziroma ali sploh) lahko izpolni zahteve iz Direktive (EU) 2016/680, še preden se začne kakršna koli obdelava s tehnologijo za prepoznavanje obraza. S skrbno analizo mora proučiti zlasti:

- kdo so posamezniki, na katere se nanašajo osebni podatki (pogosto so to več kot tisti, ki so glavni cilj za namen obdelave),
- kako so posamezniki, na katere se nanašajo osebni podatki, seznanjeni z obdelavo s tehnologijo za prepoznavanje obraza (glej oddelek 3.2.4.1),
- kako lahko posamezniki, na katere se nanašajo osebni podatki, uresničijo svoje pravice (v tem primeru je lahko spoštovanje pravic do seznanitve, do dostopa, do popravka in do omejitve še posebej zahtevno, če se tehnologija za prepoznavanje obraza uporablja za vsa preverjanja, razen za preverjanje ena na ena v neposrednem stiku s posameznikom, na katerega se nanašajo osebni podatki).

3.2.4.1 Seznanjanje posameznikov, na katere se nanašajo osebni podatki, s pravicami in informacijami v jedrnati, razumljivi in lahko dostopni obliki

85. S tehnologijo za prepoznavanje obraza nastajajo izzivi pri zagotavljanju, da so posamezniki, na katere se nanašajo osebni podatki, seznanjeni z obdelavo svojih biometričnih podatkov. To je še posebej zahtevno, kadar organ kazenskega pregona s to tehnologijo analizira videogradivo, ki izvira od tretje osebe ali ga je ta zagotovila, saj organ kazenskega pregona nima veliko možnosti, največkrat pa sploh nima možnosti, da bi posameznika, na katerega se nanašajo osebni podatki, o tem obvestil v času zbiranja (na primer z znakom na kraju samem). Vsako videogradivo, ki ni pomembno za preiskavo (ali za namen obdelave), bi bilo treba pred kakršno koli obdelavo biometričnih podatkov vedno odstraniti ali anonimizirati (na primer z zabrisanjem, brez možnosti, da se podatki obnovijo), da se prepreči

[57] Glej na primer EDPB Guidelines 01/2022 on data subject rights – Right of access (Smernice EOVP 1/2022 o pravicah posameznikov, na katere se nanašajo osebni podatki – Pravica do dostopa) in Smernice Evropskega nadzornika za varstvo podatkov 3/2019 o obdelavi osebnih podatkov z video napravami.
[58] Delovna skupina iz člena 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (Mnenje o nekaterih ključnih vprašanjih glede direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj) (Direktiva (EU) 2016/680).

tveganje, da ne bi bilo upoštevano načelo najkrajše možne hrambe podatkov iz točke e prvega odstavka 4. člena Direktive (EU) 2016/680 in ne bi bile izpolnjene obveznosti v zvezi z zagotavljanjem informacij iz drugega odstavka 13. člena Direktive (EU) 2016/680. Upravljavec mora presoditi, katere informacije bi bile pomembne za posameznika, na katerega se nanašajo osebni podatki, da ta lahko uresniči svoje pravice, in zagotoviti, da se zagotovijo potrebne informacije. Učinkovito uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, je odvisno od tega, ali upravljavec izpolnjuje svoje obveznosti v zvezi z zagotavljanjem informacij.

86. Prvi odstavek 13. člena Direktive (EU) 2016/680 določa, najmanj katere informacije je treba zagotoviti posamezniku, na katerega se nanašajo osebni podatki, na splošno. Te informacije so lahko na voljo na upravljavčevem spletnem mestu, v tiskani obliki (na primer na letaku, ki je na voljo na zahtevo) ali v drugih virih, ki so posamezniku, na katerega se nanašajo osebni podatki, zlahka dostopni. Upravljavec podatkov mora v vsakem primeru zagotoviti, da učinkovito dá na voljo vsaj naslednje informacije:

- identiteto in kontaktne podatke upravljavca, vključno s pooblaščeno osebo za varstvo podatkov,
- namen obdelave in da se podatki obdelujejo s tehnologijo za prepoznavanje obraza,
- o pravici do vložitve pritožbe pri nadzornem organu in njegove kontaktne podatke,
- o pravici, da se zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov in omejitev obdelave osebnih podatkov.

87. Poleg tega je treba v posebnih primerih, opredeljenih v nacionalni zakonodaji, ki bi morala biti v skladu z drugim odstavkom 13. člena Direktive (EU) 2016/680[59], kot je na primer obdelava s tehnologijo za prepoznavanje obraza, posamezniku, na katerega se nanašajo osebni podatki, neposredno zagotoviti naslednje informacije:

- pravno podlago za obdelavo,
- dodatne informacije, kadar se osebni podatki zbirajo brez vednosti posameznika, na katerega se nanašajo osebni podatki,
- obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja,
- kadar je to ustrezno, kategorije uporabnikov osebnih podatkov, tudi v tretjih državah ali mednarodnih organizacijah.

88. Prvi odstavek 13. člena Direktive (EU) 2016/680 določa splošne informacije, ki morajo biti na voljo javnosti, drugi odstavek 13. člena Direktive (EU) 2016/680 pa določa dodatne informacije, ki jih je treba zagotoviti zadevnemu posamezniku, na katerega se nanašajo osebni podatki, v posebnih primerih, na primer kadar se podatki zbirajo neposredno od posameznika, na katerega se nanašajo osebni podatki, ali posredno brez njegove vednosti[60]. V drugem odstavku 13. člena Direktive (EU) 2016/680 ni jasne opredelitve izraza „posebni primeri“. Nanaša pa se na primere, v katerih je treba posameznike, na katere se nanašajo osebni podatki, seznaniti z obdelavo, ki se nanje izrecno nanaša, in jim zagotoviti ustrezne informacije, da lahko učinkovito uresničujejo svoje pravice. EOVP meni, da je treba pri presoji, ali gre za poseben primer, upoštevati številne dejavnike, vključno s tem, ali se osebni podatki zbirajo

[59] Na primer prvi odstavek 56. člena nemškega zveznega zakona o varstvu podatkov med drugim določa, katere informacije je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, v tajnih operacijah.
[60] Delovna skupina iz člena 258, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (Mnenje o nekaterih ključnih vprašanjih glede direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj) (Direktiva (EU) 2016/680), str. 17–18.

brez vednosti posameznika, na katerega se nanašajo osebni podatki, saj bi bil to edini način, da se posameznikom, na katere se nanašajo osebni podatki, omogoči učinkovito uresničevanje njihovih pravic. Drugi primeri posebnih primerov bi lahko bili primeri, v katerih se osebni podatki dodatno obdelujejo v okviru postopka mednarodnega sodelovanja v kazenskih zadevah ali kadar se osebni podatki obdelujejo v okviru tajnih operacij, kot je opredeljeno v nacionalni zakonodaji. Poleg tega iz uvodne izjave 38 Direktive (EU) 2016/680 izhaja, da če se odločitve sprejemajo izključno na podlagi tehnologije za prepoznavanje obraza, morajo biti posamezniki, na katere se nanašajo osebni podatki, obveščeni o značilnostih avtomatiziranega sprejemanja odločitev. To bi pomenilo tudi, da je to posebni primer, v katerem bi bilo treba posamezniku, na katerega se nanašajo osebni podatki, zagotoviti dodatne informacije v skladu z drugim odstavkom 13. člena Direktive (EU) 2016/680[61].

89. Nazadnje, opozoriti je treba, da lahko države članice v skladu s tretjim odstavkom 13. člena Direktive (EU) 2016/680 sprejmejo zakonodajne ukrepe, ki omejujejo obveznost zagotovitve informacij v posebnih primerih za določene cilje. To velja, če in dokler je tak ukrep, ki mora spoštovati temeljne pravice in zakonite interese posameznika, na katerega se nanašajo osebni podatki, nujen in sorazmeren ukrep v demokratični družbi.

3.2.4.2 Pravica do dostopa

90. Na splošno ima posameznik, na katerega se nanašajo osebni podatki, pravico do pozitivne ali negativne potrditve kakršne koli obdelave svojih osebnih podatkov in, če je odgovor pozitiven, pravico do dostopa do osebnih podatkov kot takih, vključno z dodatnimi informacijami, kot je navedeno v 14. členu Direktive (EU) 2016/680. V zvezi s tehnologijo za prepoznavanje obraza bi moralo, kadar so biometrični podatki shranjeni in povezani z identiteto tudi z alfanumeričnimi podatki, to pristojnemu organu omogočiti, da odobri zahtevo za dostop na podlagi iskanja po teh alfanumeričnih podatkih in brez kakršne koli dodatne obdelave biometričnih podatkov drugih oseb (tj. z iskanjem v zbirki podatkov s tehnologijo za prepoznavanje obraza). Upoštevati je treba načelo najmanjšega obsega podatkov in ne sme se shranjevati več podatkov, kot je potrebno glede na namen obdelave.

3.2.4.3 Pravica do popravka osebnih podatkov

91. Ker tehnologija za prepoznavanje obraza ne zagotavlja absolutne točnosti, je še posebej pomembno, da so upravljavci pozorni na zahteve za popravek osebnih podatkov. Lahko se zgodi tudi, da je bil posameznik, na katerega se nanašajo osebni podatki, na podlagi te tehnologije uvrščen v netočno kategorijo, na primer napačno je bil uvrščen v kategorijo osumljencev na podlagi prvotne predpostavke dogajanja v videoposnetku. Tveganja za posameznike, na katere se nanašajo osebni podatki, so še posebej resna, če so taki netočni podatki shranjeni v policijski podatkovni zbirki in/ali deljeni z drugimi subjekti. Upravljavec mora shranjene podatke in sisteme za prepoznavanje obraza ustrezno popraviti, glej uvodno izjavo 47 Direktive (EU) 2016/680.

3.2.4.4 Pravica do izbrisa

92. Tehnologija za prepoznavanje obraza bo v večini primerov – če se ne bo uporabljala za preverjanje oziroma avtentikacijo ena na ena – pomenila obdelavo velikega števila biometričnih podatkov posameznikov, na katere se nanašajo osebni podatki. Zato je pomembno, da upravljavec vnaprej prouči, katere omejitve veljajo za njegov namen in potrebe, da se lahko zahteva za izbris v skladu s 16. členom Direktive (EU) 2016/680 obravnava brez nepotrebnega odlašanja (saj mora upravljavec med

[61] Upoštevati je treba razliko med navedbama „posamezniku, na katerega se nanašajo osebni podatki, dajo na voljo“ iz prvega odstavka 13. člena Direktive (EU) 2016/680 in „posamezniku, na katerega se nanašajo osebni podatki, [v posebnih primerih poleg informacij iz prvega odstavka] zagotovi“ iz drugega odstavka 13. člena Direktive (EU) 2016/680. V drugem odstavku 13. člena Direktive (EU) 2016/680 mora upravljavec zagotoviti, da informacije prispejo do posameznika, na katerega se nanašajo osebni podatki, kadar objavljene informacije na spletnem mestu ne zadostujejo.

drugim izbrisati osebne podatke, katerih obdelava presega to, kar je dovoljeno v zakonodaji, ki se uporablja in je v skladu s 4., 8. in 10. členom Direktive (EU) 2016/680).

3.2.4.5 Pravica do omejitve obdelave

93. Kadar posameznik, na katerega se nanašajo osebni podatki, izpodbija točnost podatkov in ni mogoče preveriti, ali so podatki točni ali ne (ali kadar je treba osebne podatke ohraniti za namene dokazovanja v prihodnje), mora upravljavec v skladu s 16. členom Direktive (EU) 2016/680) omejiti obdelavo osebnih podatkov zadevnega posameznika, na katerega se nanašajo osebni podatki. To postane še posebej pomembno v primeru uporabe tehnologije za prepoznavanje obraza (ta temelji na algoritmih, zato nikoli ne pokaže dokončnega rezultata) v primerih, v katerih se zbirajo velike količine podatkov, pri čemer se lahko točnost in kakovost identifikacije razlikujeta. Pri videogradivu slabe kakovosti (na primer s kraja kaznivega dejanja) se tveganje lažno pozitivnih rezultatov še poveča. Ob tem se tveganje lažno pozitivnih ali lažno negativnih rezultatov poveča tudi, če se slike obrazov oseb na seznamih nadzorovanih oseb ne posodabljajo redno. V posebnih primerih, v katerih podatkov ni mogoče izbrisati, ker obstajajo utemeljeni razlogi za sum, da bi izbris lahko vplival na zakonite interese posameznika, na katerega se nanašajo osebni podatki, bi bilo treba namesto tega podatke omejiti in jih obdelovati le za namen, ki je preprečil njihov izbris (glej uvodno izjavo 47 Direktive (EU) 2016/680).

3.2.4.6 Legitimne omejitve pravic posameznika, na katerega se nanašajo osebni podatki

94. Kar zadeva obveznosti upravljavca glede zagotovitve informacij in pravico posameznikov, na katere se nanašajo osebni podatki, do dostopa, so omejitve dovoljene le, če so določene v zakonodaji in je tak ukrep, ki mora spoštovati temeljne pravice in zakonite interese zadevnega posameznika, nujen in sorazmeren ukrep v demokratični družbi (glej tretji in četrti odstavek 13. člena ter četrti odstavek 16. člena Direktive (EU) 2016/680). Kadar se tehnologija za prepoznavanje obraza uporablja za namene kazenskega pregona, je mogoče pričakovati, da se bo uporabljala v okoliščinah, v katerih bi bilo škodljivo za postavljeni namen obveščati posameznika, na katerega se nanašajo osebni podatki, ali omogočati dostop do podatkov. To bi veljalo na primer za policijsko preiskavo kaznivega dejanja ali za zaščito nacionalne in javne varnosti.

95. Pravica do dostopa ne pomeni samodejno dostopa do vseh informacij, na primer v kazenski zadevi, v kateri se pojavijo osebni podatki posameznika. Konkreten primer, v katerem so omejitve pravice dovoljene, bi bil torej med potekom kazenske preiskave

3.2.4.7 Uresničevanje pravic prek nadzornega organa

96. Kadar obstajajo zakonite omejitve uresničevanja pravic v skladu s III. poglavjem Direktive (EU) 2016/680, lahko posameznik, na katerega se nanašajo osebni podatki, od organa za varstvo podatkov zahteva, da v imenu zadevnega posameznika uresničuje njegove pravice in v ta namen preveri zakonitost upravljavčeve obdelave podatkov. Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, obvestiti, da lahko svoje pravice uresničuje na tak način (glej 17. člen in točko g prvega odstavka 46. člena Direktive (EU) 2016/680). V zvezi s tehnologijo za prepoznavanje obraza to pomeni, da mora upravljavec zagotoviti, da so vzpostavljeni ustrezni ukrepi za obravnavo take zahteve, na primer tako, da omogoča iskanje posnetega gradiva, če posameznik, na katerega se nanašajo osebni podatki, zagotovi zadostne informacije, da se lahko ugotovi, kje so njegovi osebni podatki.

3.2.5 Druge pravne zahteve in zaščitni ukrepi

3.2.5.1 27. člen: Ocena učinka v zvezi z varstvom podatkov

97. Ocena učinka v zvezi z varstvom podatkov, preden se uporabi tehnologija za prepoznavanje obraza, je obvezna zahteva, saj lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzroči veliko tveganje za pravice in svoboščine

posameznikov. Glede na to, da uporaba tehnologije za prepoznavanje obraza vključuje sistematično avtomatsko obdelavo posebnih vrst podatkov, bi se lahko domnevalo, da bi bil v takih primerih upravljavec praviloma dolžan izvesti oceno učinka v zvezi z varstvom podatkov. Ocena učinka v zvezi z varstvom podatkov bi morala vsebovati vsaj splošni opis predvidenih dejanj obdelave, oceno nujnosti in sorazmernosti dejanj obdelave glede na namene, oceno tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ukrepe, namenjene obvladovanju teh tveganj, zaščitne ukrepe, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti. Evropski odbor za varstvo podatkov priporoča, da se rezultati takih ocen ali vsaj glavnih ugotovitev in sklepov na podlagi ocene učinka v zvezi z varstvom podatkov objavijo, in sicer kot ukrep za krepitev zaupanja in preglednosti[62].

3.2.5.2 28. člen: Predhodno posvetovanje z nadzornim organom

98. V skladu z 28. členom Direktive (EU) 2016/680 se mora upravljavec ali obdelovalec pred obdelavo osebnih podatkov posvetovati z nadzornim organom, kadar: (a) ocena učinka v zvezi z varstvom podatkov kaže, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja, ali (b) vrsta obdelave, zlasti v primeru uporabe novih tehnologij, mehanizmov ali postopkov, pomeni veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Kot je že pojasnjeno v oddelku 2.3 teh smernic, Evropski odbor za varstvo podatkov meni, da večina primerov uvajanja in uporabe tehnologije za prepoznavanje obraza že sami po sebi pomenijo veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. Zato bi se moral organ, ki uvaja tehnologijo za prepoznavanje obraza, poleg opravljene ocene učinka v zvezi z varstvom podatkov še pred namestitvijo tega sistema posvetovati s pristojnim nadzornim organom.

3.2.5.3 29. člen: Varnost obdelave

99. Zaradi edinstvene narave biometričnih podatkov ni mogoče, da bi jih posameznik, na katerega se nanašajo osebni podatki, sam spremenil, če bi bili ti podatki ogroženi, na primer zaradi kršitve varstva podatkov. Zato mora pristojni organ, ki uvaja in/ali uporablja tehnologijo za prepoznavanje obraza, posebno pozornost nameniti varnosti obdelave v skladu z 29. členom Direktive (EU) 2016/680. Organ kazenskega pregona bi moral zagotoviti zlasti, da je sistem skladen z ustreznimi standardi, in izvesti ukrepe za zaščito biometričnih predlog[63]. Ta obveznost je še pomembnejša, če organ kazenskega pregona uporablja tretjega ponudnika storitev (obdelovalca podatkov).

3.2.5.4 20. člen: Vgrajeno in privzeto varstvo podatkov

100. Cilj vgrajenega in privzetega varstva podatkov v skladu z 20. členom Direktive (EU) 2016/680 je zagotoviti, da so načela in zaščitni ukrepi za varstvo podatkov, kot sta najmanjši obseg podatkov in omejitev hrambe, vključeni v tehnologijo z ustreznimi tehničnimi in organizacijskimi ukrepi, kot je psevdonimizacija, še pred začetkom obdelave osebnih podatkov in se bodo uporabljali v celotnem življenjskem ciklu tehnologije. Glede na svojstveno veliko tveganje za pravice in svoboščine posameznikov izbira takih ukrepov ne bi smela biti odvisna samo od gospodarskih vidikov[64], namesto tega si je treba prizadevati za izvajanje najsodobnejših tehnologij za varstvo podatkov. Podobno mora organ kazenskega pregona, če namerava namestiti in uporabljati tehnologijo zunanjih ponudnikov za prepoznavanje obraza, zagotoviti, na primer s postopkom javnega naročanja, da se uvede le taka

[62] Za več informacij glej Delovna skupina za varstvo podatkov iz člena 29, Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, DS 248 rev.01.

[63] Glej na primer: ISO/IEC 24745:2022, Informacijska varnost, kibernetska varnost in varstvo zasebnosti – varstvo biometričnih podatkov.

[64] Glej uvodno izjavo 53 Direktive (EU) 2016/680.

tehnologija za prepoznavanje obraza, ki temelji na načelih vgrajenega in privzetega varstva podatkov[65]. To pomeni tudi, da preglednost delovanja tehnologije za prepoznavanje obraza ni omejena s trditvami o poslovnih skrivnostih ali pravicami intelektualne lastnine.

3.2.5.5 25. člen: Vodenje dnevnikov

101. Direktiva (EU) 2016/680 določa različne načine, s katerimi upravljavec ali obdelovalec dokaže zakonitost obdelave ter zagotovi celovitost in varnost podatkov. V zvezi s tem so sistemski dnevniki zelo koristno orodje in pomemben zaščitni ukrep za preverjanje zakonitosti obdelave, ki se izvaja interno (tj. notranje spremljanje) ali ga izvajajo zunanji nadzorni organi, na primer organi za varstvo podatkov. V skladu s 25. členom Direktive (EU) 2016/680 bi bilo treba voditi dnevnike vsaj o naslednjih dejanjih obdelave v avtomatiziranih sistemih obdelave: zbiranje, predelava, vpogled, razkritje, vključno s prenosi, kombiniranje in izbris. Poleg tega bi morali dnevniki vpogleda in razkritja omogočati utemeljitev, opredelitev datuma in časa takih dejanj ter, če je to mogoče, identifikacijo osebe, ki je vpogledala v osebne podatke ali jih razkrila, ter identiteto uporabnikov takih osebnih podatkov. Poleg tega se v okviru sistemov za prepoznavanje obraza priporoča vodenje dnevnikov o naslednjih dodatnih dejanjih obdelave (kar delno presega 25. člen Direktive (EU) 2016/680):

- spreminjanje referenčne podatkovne zbirke (dodajanje, brisanje ali posodabljanje). V dnevniku je treba hraniti kopijo ustrezne (dodane, izbrisane ali posodobljene) slike, kadar drugače ni mogoče preveriti zakonitosti ali rezultata dejanj obdelave;

- poskusi identifikacije ali preverjanja, vključno z rezultatom in oceno zaupanja. Uporabljati bi bilo treba strogo načelo najmanjšega obsega podatkov, tako da se namesto referenčne slike v dnevnikih shranjuje le identifikator slike iz referenčne podatkovne zbirke. Vodenju dnevnikov o vhodnih biometričnih podatkih bi se bilo treba izogibati, razen če je to nujno potrebno (na primer samo v primerih ujemanja);

- identiteta uporabnika, ki je zahteval poskus identifikacije ali preverjanja;

- za vse osebne podatke, shranjene v sistemskih dnevnikih, veljajo stroge omejitve namena (na primer revizije) in se ne bi smeli uporabljati za druge namene (na primer da bi lahko še vedno izvajali prepoznavanje oziroma preverjanje, vključno s sliko, ki je bila izbrisana iz referenčnih podatkovnih zbirk). Izvajati bi bilo treba varnostne ukrepe, da se zagotovi celovitost dnevnikov, za odkrivanje zlorabe dnevnikov pa so zelo priporočeni sistemi za samodejno spremljanje. Za dnevnike referenčne podatkovne zbirke morajo biti varnostni ukrepi v primeru shranjevanja slik obraza enakovredni varnostnim ukrepom referenčnih podatkovnih zbirk. Poleg tega bi bilo treba izvajati samodejne postopke, s katerimi se zagotavlja izvrševanje obdobja hrambe podatkov za dnevnike.

3.2.5.6 Četrti odstavek 4. člena: Odgovornost

102. Upravljavec mora biti zmožen dokazati skladnost obdelave z načeli iz prvega do tretjega odstavka 4. člena, prim. četrti odstavek 4. člen Direktive (EU) 2016/680). Pri tem so ključni sistematična in posodobljena dokumentacija v zvezi s sistemom (vključno s posodobitvami, nadgradnjo in algoritemskim usposabljanjem), tehnični in organizacijski ukrepi (vključno s spremljanjem delovanja sistema in morebitnim osebnim posredovanjem) ter obdelava osebnih podatkov. Za dokazovanje zakonitosti obdelave je še posebej pomembno vodenje dnevnika v skladu s 25. členom Direktive (EU) 2016/680 (prim. oddelek 3.2.5.5). Načelo odgovornosti se ne nanaša le na sistem in obdelavo,

[65] Za več informacij glej Smernice EOVP o vgrajenem in privzetem varstvu podatkov, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_sl.pdf.

temveč tudi na dokumentiranje postopkovnih zaščitnih ukrepov, kot so ocene nujnosti in sorazmernosti, ocene učinka v zvezi z varstvom podatkov ter notranja (na primer vodstvo odobri projekt ali notranje odločitve o vrednostih ocene zaupanja) in zunanja posvetovanja (na primer z organom za varstvo podatkov). V Prilogi II so številni elementi v zvezi s tem.

3.2.5.7 47. člen: Učinkovit nadzor

103. Učinkovit nadzor, ki ga izvajajo pristojni organi za varstvo podatkov, je eden najpomembnejših zaščitnih ukrepov za temeljne pravice in svoboščine posameznikov, na katere vpliva uporaba tehnologije za prepoznavanje obraza. Hkrati je zagotavljanje potrebnih človeških, tehničnih in finančnih virov, prostorov in infrastrukture vsakemu organu za varstvo podatkov osnovni pogoj za učinkovito opravljanje njihovih nalog in izvajanje pooblastil[66]. Še bolj kot število osebja, ki je na voljo, so ključni strokovno znanje in spretnosti strokovnjakov, ki morajo pokrivati zelo raznovrstna vprašanja: od kriminalističnih preiskav in policijskega sodelovanja do analitike velikih podatkov in umetne inteligence. Zato bi morale države članice zagotoviti, da imajo nadzorni organi ustrezne in zadostne vire, ki jim omogočajo izpolnjevanje njihovih pooblastil, da zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki, in pozorno spremljajo razvoj dogodkov na tem področju[67].

4 SKLEP

104. Uporaba tehnologij za prepoznavanje obraza je neločljivo povezana z obdelavo velikih količin osebnih podatkov, vključno s posebnimi vrstami podatkov. Slika obraza in, bolj na splošno, biometrični podatki so trajno in nepreklicno povezani z identiteto osebe. Zato uporaba prepoznavanja obrazov neposredno ali posredno vpliva na številne temeljne pravice in svoboščine iz Listine EU o temeljnih pravicah, ki lahko presegajo zasebnost in varstvo podatkov, kot so človekovo dostojanstvo, svoboda gibanja, svoboda zbiranja in druge. To je pomembno zlasti na področjih kazenskega pregona in kazenskega pravosodja.

105. EOVP razume potrebo organov kazenskega pregona, da morajo imeti na voljo najboljša možna orodja za hitro odkrivanje storilcev terorističnih dejanj in drugih hudih kaznivih dejanj. Vendar bi se morala taka orodja uporabljati strogo v skladu s pravnim okvirom, ki se uporablja, in le v primerih, v katerih izpolnjujejo zahteve glede nujnosti in sorazmernosti, kot so navedene v prvem odstavku 52. člena Listine. Čeprav so sodobne tehnologije lahko del rešitve, nikakor niso čudežna rešitev.

106. Nekateri primeri uporabe tehnologij za prepoznavanje obraza prinašajo nesprejemljivo velika tveganja za posameznike in družbo (omejitve). Prav zato sta EOVP in Evropski nadzornik za varstvo podatkov pozvala k njihovi splošni prepovedi[68].

107. Natančneje, biometrična identifikacija posameznikov na daljavo na javno dostopnih mestih pomeni veliko tveganje vdora v zasebno življenje posameznikov in ni primeren ukrep v demokratični družbi, saj po svoji naravi pomeni množičen nadzor. Podobno EOVP meni, da z Listino niso združljivi sistemi za prepoznavanje obraza, ki jih podpira umetna inteligenca in ki posameznike na podlagi njihovih

[66] Glej Sporočilo Komisije: Prvo poročilo o uporabi in delovanju Direktive (EU) 2016/680 o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, COM(2022) 364 final, točka 3.4.1.

[67] Glej Prispevek EOVP k vrednotenju Direktive (EU) 2016/680, ki ga je Evropska komisija opravila v skladu s členom 62 navedene direktive, odstavek 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

[68] Glej Skupno mnenje EOVP-ENVP 5/2021 o predlogu Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci), https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_sl.pdf.

biometričnih podatkov razvrščajo v skupine glede na etnično pripadnost, spol, politična stališča ali spolno usmerjenost. Poleg tega je EOVP prepričan, da je uporaba tehnologij za prepoznavanje obraza ali podobnih tehnologij za sklepanje o čustvih posameznikov zelo nezaželena in bi jo bilo treba prepovedati, po možnosti z nekaj ustrezno utemeljenimi izjemami. EOVP meni še, da obdelava osebnih podatkov v okviru kazenskega pregona, ki bi temeljila na podatkovni zbirki, ki vsebuje osebne podatke, pridobljene z množičnim in neselektivnim zbiranjem, na primer s pridobivanjem podatkov s fotografij in slik obrazov, dostopnih na spletu, zlasti tistih, ki so na voljo prek družbenih omrežij, kot taka ne bi izpolnjevala zahteve po strogi nujnosti, ki jo določa pravo Unije.

5 PRILOGE

Priloga I: Vzorec v podporo

Priloga II: Praktične smernice za organe kazenskega pregona za upravljanje projektov, pri katerih se uporablja tehnologija za prepoznavanje obraza

Priloga III: Praktični primeri

PRILOGA I: PREDLOGA ZA OPIS SCENARIJEV

(s podatkovnimi polji za vidike, obravnavane v scenariju)

Opis obdelave:

- Opis obdelave, okoliščine (povezava s kaznivimi dejanji), namen

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☐ vsi državljani ☐ obsojenci ☐ osumljenci ☐ otroci ☐ drugi ranljivi posamezniki, na katere se nanašajo osebni podatki
- Vir slike: ☐ javno dostopna mesta ☐ svetovni splet ☐ zasebni subjekt ☐ drugi posamezniki ☐ drugo: .....
- Povezava s kaznivim dejanjem: ☐ neposredna časovna povezava ☐ ni neposredne časovne povezave ☐ neposredna geografska povezava ☐ ni neposredne geografske povezave ☐ ni potrebna
- Način zajemanja informacij: ☐ na daljavo ☐ v kabini ali nadzorovanem okolju
- Okoliščine, ki vplivajo na druge temeljne pravice:
  ☐ jih ni
  Da, in sicer ☐ svoboda zbiranja
  ☐ svoboda govora
  ☐ druge:.....
- Možnosti za dodatne vire informacij o posamezniku, na katerega se nanašajo osebni podatki:
  ☐ osebni dokument ☐ uporaba javnega telefona ☐ registrska tablica vozila
  ☐ drugo: .....

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☐ podatkovne zbirke za splošne namene ☐ specifične podatkovne zbirke, povezane s področjem kriminala
- Opis, kako so bili zbrani podatki za te referenčne podatkovne zbirke (in pravna podlaga)
- Sprememba namena podatkovne zbirke (na primer: glavni cilj je bila varnost zasebne lastnine):
  ☐ DA
  ☐ NE

Algoritem:

- Vrsta obdelave: ☐ preverjanje ena na ena (avtentikacija) ☐ identifikacija s primerjanjem z več vzorci
- Pomisleki glede točnosti
- Tehnični zaščitni ukrepi

Rezultat:

- Učinek: ☐ neposreden (na primer posameznik, na katerega se nanašajo osebni podatki, je lahko prijet, zaslišan ali je zaznano diskriminatorno ravnanje)

  ☐ ni neposreden (uporablja se za statistične modele, proti posameznikom, na katere se nanašajo osebni podatki, ni resnih pravnih postopkov)

- Avtomatizirana odločitev: ☐ DA ☐ NE
- Trajanje hrambe podatkov

Pravna analiza:

- Analiza nujnosti in sorazmernosti – namen/resnost kaznivega dejanja/število oseb, ki niso vključene v obdelavo, vendar obdelava nanje vpliva.
- Vrsta predhodnega obvestila posamezniku, na katerega se nanašajo osebni podatki: ☐ ob vstopu na specifično območje

  ☐ na spletnem mestu organa kazenskega pregona na splošno

  ☐ na spletnem mestu organa kazenskega pregona za specifično obdelavo

  ☐ drugo .....
- Pravni okvir, ki se uporablja:

  ☐ Direktiva (EU) 2016/680 je bila večinoma kopirana v nacionalno pravo

  ☐ splošno nacionalno pravo, v skladu s katerim organi kazenskega pregona uporabljajo biometrične podatke

  ☐ specifično nacionalno pravo za to obdelavo (prepoznavanje obraza) za zadevni pristojni organ

  ☐ specifično nacionalno pravo za to obdelavo (avtomatizirana odločitev)

Sklep:

Splošni premisleki, ali je opisana obdelava verjetno skladna s pravom EU (in nekaj namigov o pravnih temeljnih zahtevah).

PRILOGA II: PRAKTIČNE SMERNICE ZA ORGANE KAZENSKEGA PREGONA ZA UPRAVLJANJE PROJEKTOV, PRI KATERIH SE UPORABLJA TEHNOLOGIJA ZA PREPOZNAVANJE OBRAZA

V tej prilogi je nekaj dodatnih praktičnih navodil za organe kazenskega pregona, ki nameravajo začeti izvajati projekt, pri katerem se uporablja tehnologija za prepoznavanje obraza. Zagotavlja več informacij o organizacijskih in tehničnih ukrepih, ki jih je treba upoštevati med izvajanjem projekta, navedeno pa se ne bi smelo šteti za izčrpen seznam korakov oziroma ukrepov, ki jih je treba sprejeti. Poleg tega bi jo bilo treba obravnavati v povezavi s Smernicami EOVP 3/2019 o obdelavi osebnih podatkov z video napravami[69] ter vsemi predpisi EU/EGP in smernicami EOVP v zvezi z uporabo umetne inteligence.

Ta priloga vsebuje smernice, ki temeljijo na predpostavki, da bodo organi kazenskega pregona nabavljali tehnologijo za prepoznavanje obraza (kot proizvodi, ki so splošno dostopni). Če organ kazenskega pregona načrtuje razvoj (nadaljnje usposabljanje) tehnologije za prepoznavanje obraza, veljajo dodatne zahteve za izbiranje potrebnih naborov podatkov za usposabljanje, preverjanje in preizkušanje, ki se bodo uporabljali med razvojem, ter vlog oziroma ukrepov za razvojno okolje. Podobno so lahko za proizvod, ki je splošno dostopen, potrebne dodatne prilagoditve za predvideno uporabo, v tem primeru morajo biti izpolnjene zgoraj navedene zahteve za izbiranje naborov podatkov za preizkušanje, preverjanje in usposabljanje.

Pripadnost istemu organu kazenskega pregona sama po sebi ne zagotavlja popolnega dostopa do biometričnih podatkov. Tako kot velja za druge vrste osebnih podatkov, tudi biometričnih podatkov, zbranih za zadevni namen kazenskega pregona na podlagi specifične pravne podlage, ni mogoče uporabiti brez ustrezne pravne podlage za drug namen kazenskega pregona (drugi odstavek 4. člena Direktive (EU) 2016/680). Poleg tega se razvoj orodja za prepoznavanje obraza ali usposabljanje zanj šteje za drugačen namen, zato bi bilo treba proučiti, ali je obdelava biometričnih podatkov za merjenje učinkovitosti te tehnologije ali usposabljanja zanjo, da se zaradi majhne učinkovitosti prepreči vpliv na posameznike, na katere se nanašajo osebni podatki, potrebna in sorazmerna, pri čemer je treba upoštevati prvotni namen obdelave.

1. VLOGE IN ODGOVORNOSTI

Kadar organ kazenskega pregona uporablja tehnologijo za prepoznavanje obraza za opravljanje svojih nalog, ki spadajo na področje uporabe Direktive (EU) 2016/680 (preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj itd., v skladu s 3. členom navedene direktive), se lahko šteje za upravljavca v zvezi s to tehnologijo. Vendar so organi kazenskega pregona sestavljeni iz več enot oziroma oddelkov, ki so lahko vključeni v to obdelavo, bodisi z opredelitvijo postopka uporabe te tehnologije bodisi z njeno uporabo v praksi. Zaradi posebnosti te tehnologije bo morda treba vključiti različne enote, ki bodo podpirale meritve njene učinkovitosti ali bodo izvajale nadaljnje usposabljanje v zvezi s to tehnologijo.

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

V projektu, pri katerem se uporablja tehnologija za prepoznavanje obraza, so pri organih kazenskega pregona številni deležniki[70], ki bi morda morali biti vključeni:

- najvišje vodstvo: za odobritev projekta po vzpostavitvi ravnotežja med tveganji in potencialnimi koristmi;
- pooblaščena oseba za varstvo podatkov in/ali pravni oddelek pri organu kazenskega pregona: za pomoč pri presoji zakonitosti izvajanja zadevnega projekta, pri katerem se uporablja tehnologija za prepoznavanje obraza, za pomoč pri izvajanju ocene učinka v zvezi z varstvom podatkov ter za zagotavljanje spoštovanja in uresničevanja pravic posameznikov, na katere se nanašajo osebni podatki;
- lastnik postopka: deluje kot specifična enota pri pristojnem organu kazenskega pregona za razvoj projekta, odloča o podrobnostih projekta, pri katerem se uporablja tehnologija za prepoznavanje obraza, vključno z zahtevami glede učinkovitosti sistema, odločanje o ustrezni metriki pravičnosti, opredeli oceno zaupanja[71], opredeli sprejemljive pragove pristranskosti, opredeli potencialna tveganja, ki jih projekt, pri katerem se uporablja tehnologija za prepoznavanje obraza, ustvarja v zvezi s pravicami in svoboščinami posameznikov (na podlagi posvetovanja tudi s pooblaščeno osebo za varstvo podatkov ter oddelkom za informatiko in umetno inteligenco in/ali podatkovno znanost (glej v nadaljevanju)) ter jih predstavi najvišjemu vodstvu. Lastnik postopka se bo pred odločitvijo o podrobnostih projekta, pri katerem se uporablja tehnologija za prepoznavanje obraza, posvetoval tudi z upravljavcem referenčne podatkovne zbirke, da bi razumel namen uporabe referenčne podatkovne zbirke in tudi tehnične podrobnosti. V primeru vnovičnega usposabljanja v zvezi z nabavljeno tehnologijo za prepoznavanje obraza bo lastnik postopka odgovoren tudi za izbiro nabora podatkov za usposabljanje. Lastnik postopka je kot enota, odgovorna za pripravo in odločanje o podrobnostih projekta, odgovoren za izvedbo ocene učinka v zvezi z varstvom podatkov;
- oddelek za informatiko in umetno inteligenco in/ali podatkovno znanost: za pomoč pri izvedbi ocene učinka v zvezi z varstvom podatkov, za pojasnitev metrike, ki je na voljo za merjenje učinkovitosti, pravičnosti[72] in morebitne pristranskosti sistema, za uvajanje tehnologije in izvajanje tehničnih zaščitnih ukrepov, da se preprečijo nepooblaščen dostop do zbranih podatkov, kibernetski napadi in podobno. V primeru vnovičnega usposabljanja v zvezi z nabavljeno tehnologijo za prepoznavanje obraza bo ta oddelek usposobil sistem na podlagi nabora podatkov za usposabljanje, ki ga zagotovi lastnik postopka. Ta oddelek bo odgovoren tudi za vzpostavitev ukrepov za ublažitev tveganj, ki so jih skupaj opredelili lastniki postopkov (na primer specifična tveganja v zvezi z umetno inteligenco, kot so napadi na sklepanje na podlagi modelov);
- končni uporabniki (na primer policisti na terenu ali v forenzičnih laboratorijih): za izvajanje primerjave s podatkovno zbirko, za kritični pregled rezultatov ob upoštevanju predhodnih dokazov, poleg tega lastniku postopka zagotovijo povratne informacije o lažno pozitivnih rezultatih in znakih morebitne diskriminacije;
- upravitelj referenčne podatkovne zbirke: specifična enota pri pristojnem organu kazenskega pregona, odgovorna za zbiranje in upravljanje referenčne podatkovne zbirke, tj. zbirke podatkov,

[70] V nadaljevanju so navedene vloge različnih deležnikov in njihove odgovornosti pri projektu, pri katerem se uporablja tehnologija za prepoznavanje obraza. Čeprav opisi vlog v tej prilogi niso zapisani povsem natančno, mora vsak organ kazenskega pregona opredeliti in dodeliti podobne vloge v skladu s svojo organizacijo. Možno je, da ima enota več kot eno vlogo, na primer lastnik postopka in upravljavec referenčne podatkovne zbirke ali lastnik postopka ter oddelek za informatiko in umetno inteligenco in/ali podatkovno znanost (če ima enota, v kateri je lastnik postopka, vse potrebno tehnično znanje).

[71] Ocena zaupanja je stopnja zaupanja napovedi (ujemanja) v obliki verjetnosti. Če se primerjata na primer dve predlogi, velja 90-odstotna gotovost, da obe pripadata isti osebi. Ocena zaupanja se razlikuje od učinkovitosti tehnologije za prepoznavanje obraza, vendar vpliva na učinkovitost. Višji kot je prag zaupanja, manj je lažno pozitivnih in več je lažno negativnih rezultatov na podlagi te tehnologije.

[72] Pravičnost po definiciji pomeni, da ni nepoštene, nezakonite diskriminacije, na primer pristranskost na podlagi spolne usmerjenosti ali rasne pripadnosti.

s katero se bodo primerjale slike, to vključuje tudi brisanje slik obraza po določenem obdobju hrambe. Taka podatkovna zbirka je lahko ustvarjena izrecno za predvideni projekt, pri katerem se uporablja tehnologija za prepoznavanje obraza, ali je bila vzpostavljena že prej, za združljive namene. Upravljavec referenčne podatkovne zbirke je odgovoren za opredelitev, kdaj in v katerih okoliščinah se lahko slike obraza shranjujejo, ter za določitev zahtev za njihovo hrambo (v skladu z obdobjem ali drugimi merili).

Ker večina primerov uvajanja in uporabe tehnologije za prepoznavanje obraza že sama po sebi pomeni veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, bi moral biti vključen tudi nadzorni organ za varstvo podatkov v okviru predhodnega posvetovanja, ki se zahteva v skladu z 28. členom Direktive (EU) 2016/680.

2. ZAČETEK/PRED NAROČILOM SISTEMA ZA PREPOZNAVANJE OBRAZA

Lastnik postopka pri organu kazenskega pregona bi moral najprej jasno razumeti postopek oziroma postopke, ki sledi(-jo) uporabi tehnologije za prepoznavanje obraza (primer(-i) uporabe), in zagotoviti, da je pripravljena pravna podlaga za utemeljitev predvidenega primera uporabe. Na podlagi tega mora:

- formalno opisati primer uporabe. Opisati je treba težavo, ki jo je treba rešiti, in način, kako bo tehnologija za prepoznavanje obraza zagotovila rešitev, ter navesti pregled postopka (naloge), v katerem se bo to uporabilo. V zvezi s tem bi morali organi kazenskega pregona dokumentirati vsaj[73]:
  - vrste osebnih podatkov, shranjenih v postopku,
  - cilje in konkretne namene, za katere se bo uporabljala tehnologija za prepoznavanje obraza, vključno z možnimi posledicami za posameznika, na katerega se nanašajo osebni podatki, po ujemanju,
  - kdaj in kako se bodo zbirale slike obraza (vključno z informacijami o okoliščinah tega zbiranja, na primer na izhodu za vkrcanje na letališču, z videoposnetki varnostnih kamer pred trgovino, kjer je bilo storjeno kaznivo dejanje, itd., in kategorijami posameznikov, na katere se nanašajo osebni podatki in katerih biometrični podatki se bodo obdelovali),
  - podatkovno zbirko, s katero se bodo primerjale slike (referenčna podatkovna zbirka), ter informacije o tem, kako je bila ustvarjena, kako obsežna je in kakšna je kakovost biometričnih podatkov, ki jih vsebuje,
  - akterje organa kazenskega pregona, ki bodo pooblaščeni za uporabo sistema za prepoznavanje obraza in delovanje v skladu z njim v okviru kazenskega pregona (njihove profile in pravice dostopa mora opredeliti lastnik postopka),
  - predvideno obdobje hrambe vhodnih podatkov ali trenutek, ki bo določil konec tega obdobja (na primer zaključek ali ustavitev kazenskega postopka v skladu z nacionalnim procesnim pravom, za katerega so bili podatki prvotno zbrani), ter morebitne nadaljnje ukrepe (izbris teh podatkov, anonimizacija in uporaba v statistične ali raziskovalne namene itd.),
  - vodenje dnevnika in dostopnost dnevnikov ter shranjenih zapisov,
  - merila učinkovitosti (na primer točnost, natančnost, priklic, ocena F1) in njihove najnižje sprejemljive mejne vrednosti[74],

[73] V Prilogi I je seznam elementov, ki so upravljavcu v pomoč pri opisu primera, pri katerem se uporablja tehnologija za prepoznavanje obraza.

[74] Možne so različne metrike za oceno učinkovitosti sistema za prepoznavanje obraza. Vsaka metrika zagotavlja drugačen pogled na rezultate sistema, uspešnost pri zagotavljanju ustrezne podobe o tem, ali sistem za

- oceno, koliko ljudi bo vključenih v uporabo tehnologije za prepoznavanje obraza, v katerem obdobju ali ob kateri priložnosti;

- izvesti oceno nujnosti in sorazmernosti[75]. Dejstvo, da ta tehnologija obstaja, ne bi smelo biti glavni razlog za njeno uporabo. Lastnik postopka mora najprej proučiti, ali obstaja ustrezna pravna podlaga za predvideno obdelavo. V ta namen se je treba posvetovati s pooblaščeno osebo za varstvo podatkov in pravno službo. Glavni razlog za uvedbo tehnologije za prepoznavanje obraza mora biti, da je to nujna in sorazmerna rešitev za specifično opredeljeno težavo organa kazenskega pregona. To je treba proučiti glede na namen oziroma resnost kaznivega dejanja oziroma število oseb, ki niso vpletene, vendar nanje vpliva sistem za prepoznavanje obraza. Pri presoji zakonitosti bi bilo treba upoštevati vsaj Direktivo (EU) 2016/680[76], Splošno uredbo o varstvu podatkov[77, 78], kateri koli veljavni pravni okvir o umetni inteligenci[79] in vse spremljajoče smernice, ki so jih zagotovili nadzorni organi za varstvo podatkov (kot so Smernice EOVP 3/2019 o obdelavi osebnih podatkov z video napravami[80]). Te akte zakonodaje EU je treba vedno upoštevati skupaj z nacionalnimi zahtevami, ki se uporabljajo, zlasti na področju kazenskega procesnega prava. Pri presoji sorazmernosti bi bilo treba opredeliti temeljne pravice posameznikov, na katere se nanašajo osebni podatki in na katere bi to lahko vplivalo (poleg zasebnosti in varstva podatkov). Poleg tega bi bilo treba opisati in upoštevati morebitne omejitve (ali to, da ni omejitev), ki veljajo v primeru uporabe sistema za prepoznavanje obraza. Na primer, če bo sistem deloval neprekinjeno ali začasno in če bo uporaba omejena na geografsko območje;
- izvesti oceno učinka v zvezi z varstvom podatkov [81]. Izvesti bi bilo treba oceno učinka v zvezi z varstvom podatkov, saj lahko uporaba tehnologije za prepoznavanje obraza na področju kazenskega pregona povzroči veliko tveganje za pravice in svoboščine posameznikov[82]. Ocena

prepoznavanje obraza deluje dobro ali ne, pa je odvisna od primera uporabe tehnologije za prepoznavanje obraza. Če je poudarek na doseganju visokih odstotkov pravilnega ujemanja obraza, se lahko uporabijo metrike, kot sta točnost in priklic. Vendar te metrike ne merijo, kako dobro se s tehnologijo za prepoznavanje obraza obravnavajo negativni primeri (v koliko primerih je bilo ujemanje v sistemu napačno). Lastnik postopka, ki mu podporo zagotavlja oddelek za informatiko in umetno inteligenco ter podatkovno znanost, bi moral biti zmožen določiti zahteve glede učinkovitosti in nato izraziti v najprimernejši metriki v skladu s primerom uporabe tehnologije za prepoznavanje obraza.

[75] Nadaljnje ukrepe za upoštevanje nujnosti je mogoče obravnavati glede na prilagajanje in uporabo sistema, zato se lahko opis primera uporabe med presojo nujnosti in sorazmernosti tudi nekoliko spremeni.

[76] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

[77] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

[78] V primerih, ko bi bilo treba v okviru znanstvenega projekta, namenjenega raziskovanju uporabe tehnologije za prepoznavanje obraza, obdelati osebne podatke, vendar taka obdelava ne bi spadala v področje uporabe tretjega odstavka 4. člena Direktive (EU) 2016/680, bi se na splošno uporabljala Splošna uredba o varstvu podatkov (drugi odstavek 9. člena Direktive (EU) 2016/680). V primeru pilotnih projektov, ki bi jim sledili ukrepi kazenskega pregona, bi se še vedno uporabljala Direktiva (EU) 2016/680.

[79] Pripravljen je na primer predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA O DOLOČITVI HARMONIZIRANIH PRAVIL O UMETNI INTELIGENCI (AKT O UMETNI INTELIGENCI) IN SPREMEMBI NEKATERIH ZAKONODAJNIH AKTOV UNIJE, vendar ta še ni uveljavljena kot uredba.

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

[81] Dodatne smernice o ocenah učinka v zvezi z varstvom podatkov so na voljo v dokumentu Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679, WP 248 rev.01, na voljo na naslovu: https://ec.europa.eu/newsroom/article29/items/611236, in v zbirki orodij Evropskega nadzornika za varstvo podatkov o odgovornosti na terenu, del II, na voljo na naslovu: https://edps.europa.eu/node/4582_en.

[82] Tehnologija za prepoznavanje obraza, odvisno od primera uporabe, lahko spada med naslednja merila, ki so razlog za obdelavo z velikim tveganjem (iz smernic o oceni učinka v zvezi z varstvom podatkov, DS 248 rev.01):

učinka v zvezi z varstvom podatkov bi morala vsebovati zlasti: splošen opis predvidenih postopkov obdelave[83], oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki[84], ukrepe, predvidene za obvladovanje teh tveganj, zaščitne ukrepe, varnostne ukrepe in mehanizme za zagotavljanje varstva osebnih podatkov in dokazovanje skladnosti. Ocena učinka v zvezi z varstvom podatkov je stalen proces, zato bi bilo treba v vsaki fazi projekta dodati morebitne nove elemente obdelave in posodobiti oceno tveganja;

- pridobiti odobritev najvišjega vodstva s pojasnitvijo tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki (iz primera uporabe in tehnologije), ter ustreznih načrtov za obvladovanje tveganj.

3. MED NAROČANJEM IN PRED UVEDBO TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZA

- Določite merila za izbiro tehnologije za prepoznavanje obraza (algoritem). Lastnik postopka bi moral določiti merila za izbiro algoritma ob pomoči oddelka za informatiko in umetno inteligenco in/ali podatkovno znanost. V praksi bi to vključevalo metrike pravičnosti in učinkovitosti, opredeljene v opisu primera uporabe. Taka merila bi morala vključevati tudi informacije v zvezi s podatki, uporabljenimi z algoritmom, v zvezi s katerim je potekalo usposabljanje. Nabor podatkov za usposabljanje, preizkušanje in preverjanje mora v zadostni meri vključevati vzorce vseh značilnosti posameznikov, na katere se nanašajo osebni podatki in katerih podatki bodo obdelani s tehnologijo za prepoznavanje obraza (na primer starost, spol in rasa), da se zmanjša pristranskost. Ponudnik tehnologije za prepoznavanje obraza bi moral zagotoviti informacije in metrike o naborih podatkov za usposabljanje, preizkušanje in preverjanje ter opisati ukrepe, sprejete za merjenje in zmanjšanje možnosti za morebitno nezakonito diskriminacijo in pristranskost. Lastnik postopka mora, kadar je mogoče, preveriti, ali je ponudnik imel pravno podlago za uporabo tega nabora podatkov za namene usposabljanja v zvezi z algoritmi (na podlagi informacij, ki jih bo ponudnik dal na voljo). Poleg tega bi moral lastnik postopka zagotoviti, da ponudnik tehnologije za prepoznavanje obraza uporablja varnostne standarde, povezane z biometričnimi podatki, kot je ISO/IEC 24745, ki zagotavlja smernice za zaščito biometričnih podatkov v skladu z raznimi zahtevami glede zaupnosti, celovitosti in obnovljivosti oziroma preklica med shranjevanjem in prenosom, ter zahteve in smernice za varno upravljanje in obdelavo biometričnih informacij, ki upoštevata zasebnost.

- Znova izvedite usposabljanje v zvezi z algoritmom (po potrebi). Lastnik postopka bi moral zagotoviti, da je del naročenih storitev tudi natančno prilagajanje sistema za prepoznavanje obraza, da se doseže večja točnost, preden se začne uporabljati. Če je za to, da se dosežejo metrike točnosti, potrebno dodatno usposabljanje v zvezi z nabavljeno tehnologijo za prepoznavanje obraza, se mora lastnik postopka, poleg tega, da sprejme odločitev o vnovičnem usposabljanju, ob pomoči oddelka za informatiko in umetno inteligenco in/ali podatkovno znanost odločiti o

sistematično spremljanje, obdelava podatkov v velikem obsegu, ujemanje ali združevanje naborov podatkov, inovativna uporaba ali uporaba novih tehnoloških ali organizacijskih rešitev.

[83] Tudi opis obdelave ter ocena nujnosti in sorazmernosti, kot je že navedeno v zgornjih korakih, so poleg ocene tveganja del ocene učinka v zvezi z varstvom podatkov. Po potrebi bo v oceni učinka v zvezi z varstvom podatkov naveden podrobnejši opis tokov osebnih podatkov.

[84] Analiza tveganj za posameznike, na katere se nanašajo osebni podatki, bi morala vključevati tveganja v zvezi z lokacijo, kjer se primerjajo slike obraza (lokalno oziroma na daljavo), tveganja v zvezi z obdelovalci oziroma podobdelovalci, in tveganja, specifična za strojno učenje, kadar se to uporablja (na primer zastrupljanje podatkov, nasprotovalni primeri).

ustreznem, reprezentativnem naboru podatkov, ki ga je treba uporabiti, in preveriti zakonitost te uporabe za podatke.

- Opredelite ustrezne zaščitne ukrepe, s katerimi se obravnavajo tveganja, povezana z varnostjo, pristranskostjo in nizko učinkovitostjo. To vključuje vzpostavitev postopka za spremljanje tehnologije za prepoznavanje obraza, ko se začne uporabljati (vodenje dnevnika in povratne informacije za točnost in pravičnost rezultatov). Poleg tega je treba zagotoviti, da so tveganja, specifična za nekatere sisteme za strojno učenje in za prepoznavanje obraza (na primer zastrupitev podatkov, nasprotovalni primeri, inverzija modela, sklepanje na podlagi zasnove), opredeljena, izmerjena in se obvladujejo. Lastnik postopka bi moral opredeliti tudi ustrezne zaščitne ukrepe, s katerimi bi zagotovil, da se bodo upoštevale zahteve glede hrambe biometričnih podatkov, vključenih v nabor podatkov za vnovično usposabljanje.
- Dokumentirajte sistem za prepoznavanje obraza. To bi moralo vključevati splošni opis sistema za prepoznavanje obraza, podroben opis elementov tega sistema in postopka za njegovo vzpostavitev, podrobne informacije o spremljanju, delovanju in nadzoru sistema za prepoznavanje obraza ter podroben opis njegovih tveganj in ukrepov za njihovo obvladovanje. Elementi, vključeni v to dokumentacijo, bodo vključevali glavne elemente opisa sistema za prepoznavanje obraza iz prejšnjih faz (glej zgoraj), ob tem bodo razširjeni z informacijami v zvezi s spremljanjem učinkovitosti in uporabo sprememb v sistemu, vključno z morebitnimi posodobitvami različic in/ali vnovičnim usposabljanjem.
- Pripravite priročnike za uporabnike, v katerih pojasnite tehnologijo in primere uporabe. V teh morajo biti jasno pojasnjeni vsi scenariji in temeljni pogoji, v skladu s katerimi se bo uporabljala tehnologija za prepoznavanje obraza.
- Usposobite končne uporabnike o tem, kako se tehnologija uporablja. Na takih usposabljanjih je treba pojasniti zmogljivosti in omejitve tehnologije, da bodo lahko uporabniki razumeli okoliščine, v katerih jo je treba uporabiti, in primere, v katerih je lahko netočna. Taka usposabljanja bodo v pomoč tudi pri obvladovanju tveganj, povezanih z nepreverjanjem oziroma kritiziranjem rezultatov algoritma.
- Posvetujte se z nadzornim organom za varstvo podatkov, v skladu s točko b prvega odstavka 28. člena Direktive (EU) 2016/680. Zagotovite informacije v skladu s 13. členom Direktive (EU) 2016/680, da se posameznike, na katere se nanašajo osebni podatki, obvesti o obdelavi in o njihovih pravicah. Ta obvestila morajo biti za posameznike, na katere se nanašajo osebni podatki, ne preveč zahtevna, da lahko razumejo obdelavo, poleg tega morajo vsebovati razlago osnovnih elementov tehnologije, vključno s stopnjami točnosti, nabori podatkov za usposabljanje in ukrepi, sprejetimi za preprečevanje diskriminacije in slabe natančnosti algoritma.

4. PRIPOROČILA PO UVEDBI TEHNOLOGIJE ZA PREPOZNAVANJE OBRAZA

- Zagotovite osebno posredovanje in nadzor rezultatov. Nikoli ne sprejmite nobenega ukrepa v zvezi s posameznikom izključno na podlagi rezultata tehnologije za prepoznavanje obraza (to bi pomenilo kršitev 11. člena Direktive (EU) 2016/680 – avtomatizirano sprejemanje posameznih odločitev, ki ima pravne ali druge podobne učinke na posameznika, na katerega se nanašajo osebni podatki). Zagotovite, da bo uradnik pri organu kazenskega pregona pregledal rezultate tehnologije za prepoznavanje obraza. Zagotovite tudi, da se uporabniki pri organu kazenskega pregona izogibajo pristranskosti zaradi avtomatizacije, in sicer s proučitvijo nasprotujočih si informacij in kritičnim vrednotenjem rezultatov te tehnologije. Za to sta pomembna stalno usposabljanje in ozaveščanje končnih uporabnikov, najvišje vodstvo pa mora zagotoviti ustrezne človeške vire za izvajanje učinkovitega nadzora. To pomeni, da je treba vsakemu agentu zagotoviti

dovolj časa, da kritično ovrednoti rezultate te tehnologije. Evidentirajte, izmerite in proučite, v kolikšnem obsegu osebni nadzor spremeni prvotno odločitev te tehnologije.

- Spremljajte in obravnavajte spremembo modela tehnologije za prepoznavanje obraza (zmanjšanje učinkovitosti), po tem ko je model v redni rabi.
- Vzpostavite postopek za vnovično presojo tveganj in varnostnih ukrepov, in to redno ter ob vsaki spremembi tehnologije ali primera uporabe.
- Dokumentirajte vsako spremembo sistema v njegovem celotnem življenjskem ciklu (na primer nadgradnje, vnovično usposabljanje).
- Vzpostavite postopek in opredelite s tem povezane tehnične zmogljivosti za obravnavanje zahtevkov za dostop, ki jih vložijo posamezniki, na katere se nanašajo osebni podatki. Tehnične zmogljivosti za pridobivanje podatkov, če bi jih bilo treba zagotoviti posameznikom, na katere se nanašajo osebni podatki, morajo biti vzpostavljene, še preden se pojavi taka zahteva.
- Zagotovite, da so vzpostavljeni postopki za primere kršitev varnosti podatkov. V primeru kršitve varstva osebnih podatkov, ki vključuje biometrične podatke, bodo tveganja verjetno velika. V tem primeru bi morali biti vsi vključeni uporabniki seznanjeni z ustreznimi postopki, ki jih je treba upoštevati, ob tem bi bilo treba nemudoma obvestiti pooblaščeno osebo za varstvo podatkov in posameznike, na katere se nanašajo osebni podatki.

PRILOGA III: PRAKTIČNI PRIMERI

Obstaja veliko praktičnih okoliščin in namenov uporabe tehnologij za prepoznavanje obraza, na primer v nadzorovanih okoljih, kot so mejni prehodi, navzkrižno preverjanje s podatki iz policijskih podatkovnih zbirk ali z osebnimi podatki, ki jih je posameznik, na katerega se podatki nanašajo, sam objavil, posnetki kamer v živo (prepoznavanje obraza v živo) itd. Zato se tveganja za varstvo osebnih podatkov ter drugih temeljnih pravic in svoboščin v različnih primerih uporabe zelo razlikujejo. Da bi olajšali presojo nujnosti in sorazmernosti, ki bi morala biti izvedena, še preden se sprejme odločitev o morebitni uvedbi prepoznavanja obrazov, sedanje smernice zagotavljajo neizčrpen seznam možnih uporab tehnologije za prepoznavanje obraza na področju kazenskega pregona.

Predstavljeni in proučeni scenariji temeljijo na **hipotetičnih** okoliščinah, njihov namen pa je ponazoriti nekatere konkretne uporabe tehnologije za prepoznavanje obraza, zagotoviti pomoč pri obravnavi posameznih primerov in določiti splošni okvir. Ti niso izčrpni in ne posegajo v katere koli potekajoče ali prihodnje postopke nacionalnega nadzornega organa v zvezi z oblikovanjem, preizkušanjem ali izvajanjem tehnologij za prepoznavanje obraza. Predstavitev teh scenarijev bi se morala uporabiti le kot ponazoritev smernic za oblikovalce politik, zakonodajalce in organe kazenskega pregona, ki so že navedene v tem dokumentu, pri oblikovanju in načrtovanem izvajanju tehnologij za prepoznavanje obrazov, da se zagotovi popolna skladnost s pravnim redom EU na področju varstva osebnih podatkov. V zvezi s tem bi bilo treba upoštevati, da lahko tudi v podobnih primerih uporabe tehnologij za prepoznavanje obraza obstoj ali neobstoj nekaterih elementov privede do drugačnega rezultata presoje nujnosti in sorazmernosti.

1 SCENARIJ 1

1.1. Opis

Sistem avtomatiziranega mejnega nadzora omogoča avtomatizirano prehajanje meje s preverjanjem pristnosti biometrične slike, shranjene v elektronski potni listini državljanov EU in drugih potnikov, ki prečkajo mejni prehod, ter ugotovi, da je potnik zakoniti imetnik listine.

Tako preverjanje oziroma avtentikacija vključuje le prepoznavanje obraza ena na ena in se izvaja v nadzorovanem okolju (na primer: letališki elektronski prehod). Biometrični podatki potnika, ki prehaja mejni prehod, se zajamejo, ko je izrecno pozvan, naj na elektronskem prehodu pogleda v kamero, in se primerjajo s podatki iz predloženega dokumenta (potnega lista, osebne izkaznice itd.), ki se izda v skladu s specifičnimi tehničnimi zahtevami.

Čeprav obdelava v takih primerih načeloma ne spada na področje uporabe Direktive (EU) 2016/680, se lahko rezultat preverjanja uporabi tudi za ujemanje (alfanumeričnih) podatkov osebe s podatkovnimi zbirkami organov kazenskega pregona v okviru nadzora meje in tako lahko vključuje ukrepe s precejšnjim pravnim učinkom za posameznika, na katerega se nanašajo osebni podatki, na primer prijetje na podlagi razpisa ukrepa v SIS. V specifičnih okoliščinah se lahko biometrični podatki uporabljajo tudi za iskanje ujemanj v podatkovnih zbirkah organov kazenskega pregona (v takem primeru bi se v tem koraku opravila identifikacija s primerjanjem z več vzorci).

Rezultat obdelave biometrične slike neposredno vpliva na posameznika, na katerega se nanašajo osebni podatki: prehod meje omogoča le v primeru uspešnega preverjanja. V primeru neuspešne identifikacije morajo mejni policisti opraviti drugo preverjanje, s čimer se prepričajo, da je posameznik, na katerega se nanašajo osebni podatki, drugačen od tistega, čigar slika je v identifikacijskem dokumentu.

Če se ugotovi, da je v SIS razpisan ukrep ali je razpisan nacionalni ukrep, morajo mejni policisti opraviti drugo preverjanje in potrebna nadaljnja preverjanja ter nato sprejeti vse potrebne ukrepe, na primer prijeti osebo ali obvestiti zadevne organe.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ vsi posamezniki, ki prehajajo meje
- Vir slike: ☒ drugo (identifikacijski dokument)
- Povezava s kaznivim dejanjem: ☒ ni potrebna
- Način zajemanja informacij: ☒ v kabini ali nadzorovanem okolju
- Okoliščine, ki vplivajo na druge temeljne pravice: Da, in sicer: ☒ pravica do prostega gibanja ☒ pravica do azila

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☒ specifične podatkovne zbirke, povezane z mejnim nadzorom

Algoritem:

- Vrsta preverjanja: ☒ preverjanje ena na ena (avtentikacija)

Rezultat:

- Učinek: ☒ neposreden (posamezniku, na katerega se nanašajo osebni podatki, je vstop dovoljen ali zavrnjen)
- Avtomatizirana odločitev: ☒ Da

1.2. Pravni okvir, ki se uporablja

Od leta 2004 morajo potni listi in drugi potovalni dokumenti, ki jih izdajo države članice, v skladu z Uredbo Sveta (ES) št. 2252/2004[85] vsebovati biometrično sliko obraza, shranjeno v elektronskem čipu, vgrajenem v dokument.

Zahteve za mejne kontrole oseb na zunanjih mejah določa Zakonik o schengenskih mejah[86]. Za državljane EU in druge osebe, ki uživajo pravico do prostega gibanja v skladu s pravom Unije, bi morala minimalna preverjanja vključevati preverjanje njihovih potnih listin, po potrebi z uporabo tehničnih naprav. Zakonik o schengenskih mejah je bil pozneje spremenjen z Uredbo (EU) 2017/2225,[87] ki je med drugim uvedla opredelitve izrazov „elektronski prehod“, „avtomatizirani sistem nadzora meje“ in „samopostrežni sistem“ ter možnost obdelave biometričnih podatkov za izvajanje mejnih kontrol.

Zato je mogoče domnevati, da velja jasna in predvidljiva pravna podlaga, s katero je dovoljena ta oblika obdelave osebnih podatkov. Poleg tega je pravni okvir sprejet na ravni Unije in se neposredno uporablja v državah članicah.

1.3. Nujnost in sorazmernost – namen oziroma resnost kaznivega dejanja

Preverjanje identitete državljanov EU v okviru avtomatiziranega nadzora meja z uporabo njihove biometrične slike je sestavni del mejnih kontrol na zunanjih mejah EU. Zato je to neposredno povezano z varnostjo meja in se uporablja za izpolnjevanje cilja splošnega interesa, ki ga priznava Unija. Poleg tega avtomatizirani sistemi mejnega nadzora pomagajo pospešiti obdelavo podatkov potnikov in zmanjšati tveganje človeških napak. Ob tem so področje uporabe, obseg in intenzivnost poseganja v

[85] Uredba Sveta (ES) št. 2252/2004 z dne 13. decembra 2004 o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice.
[86] Uredba (EU) št. 2016/399 Evropskega parlamenta in Sveta z dne 9. marca 2016 o Zakoniku Unije o pravilih, ki urejajo gibanje oseb prek meja (Zakonik o schengenskih mejah).
[87] Uredba (EU) 2017/2225 Evropskega parlamenta in Sveta z dne 30. novembra 2017 o spremembi Uredbe (EU) 2016/399 glede uporabe sistema vstopa/izstopa.

tem scenariju veliko bolj omejeni v primerjavi z drugimi oblikami prepoznavanja obraza. Kljub temu obdelava biometričnih podatkov ustvarja dodatna tveganja za posameznike, na katere se nanašajo osebni podatki, ki jih mora pristojni organ, ki uvaja in upravlja tehnologijo za prepoznavanje obraza, ustrezno obravnavati in obvladovati.

1.4. Sklep

Preverjanje identitete državljanov EU v okviru avtomatiziranega nadzora meja je nujen in sorazmeren ukrep, če so vzpostavljeni ustrezni zaščitni ukrepi, zlasti uporaba načel omejitve namena, kakovosti podatkov, preglednosti in visoke ravni varnosti.

2 SCENARIJ 2

2.1. Opis

Organi kazenskega pregona vzpostavijo sistem identifikacije otrok žrtev ugrabitve. Pooblaščeni policist lahko pod strogimi pogoji primerja biometrične podatke otroka, za katerega se sumi, da je ugrabljen, s podatkovno zbirko o otrocih žrtvah ugrabitev, in sicer izključno z namenom identifikacije mladoletnikov, ki bi lahko ustrezali opisu pogrešanega otroka, za katerega sta bila uvedena preiskava in izdan razpis ukrepa.

Zadevna obdelava bi bila primerjava slike obraza ali slike posameznika, ki bi lahko ustrezala opisu pogrešanega otroka, s slikami, shranjenimi v podatkovni zbirki. Tovrstna obdelava bi se izvajala v specifičnih primerih, ne sistematično.

Podatkovna zbirka, na podlagi katere se bo izvajala primerjava, vsebuje slike pogrešanih otrok, za katere je bil prijavljen sum ugrabitve, ki ogroža otrokovo življenje ali telesno celovitost, in za katere je bila pri sodnem organu uvedena kazenska preiskava ter je bil izdan razpis ukrepa zaradi ugrabitve otroka. Podatki se zbirajo v okviru postopkov, ki jih določi pristojni organ kazenskega pregona, tj. policisti, ki so pooblaščeni za izvajanje nalog pravosodne policije. Vrste shranjenih osebnih podatkov so:

- identiteta, vzdevek, privzeto ime, sorodstveno razmerje, državljanstvo, naslovi, e-naslovi, telefonske številke;
- datum in kraj rojstva:
- informacije o starševstvu;
- fotografija s tehničnimi značilnostmi, ki omogočajo uporabo naprave za prepoznavanje obraza, in druge fotografije.

Rezultate primerjave mora pregledati in preveriti tudi pooblaščeni uradnik, da prejšnje dokaze potrdi z rezultatom primerjave in izključi morebitne lažno pozitivne rezultate.

Slike otrok in osebni podatki se lahko hranijo le za čas trajanja razpisa ukrepa in jih je treba izbrisati takoj po zaključku ali koncu kazenskega postopka v skladu z nacionalnimi postopki, za katere so bili vneseni v podatkovno zbirko.

Čeprav je hramba biometričnih podatkov v podatkovni zbirki lahko predvidena za razmeroma dolgo obdobje in je to opredeljeno v skladu z nacionalno zakonodajo, uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki, zlasti pravic do popravka in do izbrisa, zagotavlja dodatno jamstvo za omejitev poseganja v pravico zadevnih posameznikov, na katere se nanašajo osebni podatki, do varstva osebnih podatkov.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ otroci
- Vir slike: ☒ drugo: ni vnaprej določeno, domnevna žrtev ugrabitve otroka
- Povezava s kaznivim dejanjem: ☒ ni neposredne časovne povezave ☒ ni neposredne geografske povezave
- Način zajemanja informacij: ☒ v kabini ali nadzorovanem okolju
- Okoliščine, ki vplivajo na druge temeljne pravice: ☒ Da, in sicer: ☒ druge

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost ☒ specifična podatkovna zbirka

Algoritem:

- Vrsta preverjanja: ☒ identifikacija s primerjanjem z več vzorci

Rezultat:

- Učinek: ☒ neposreden
- Avtomatizirana odločitev: ☒ NE, obvezen pregled, ki ga opravi pooblaščena oseba

Pravna analiza:

- Pravni okvir, ki se uporablja: ☒ specifično nacionalno pravo za to obdelavo prepoznavanje obraza)

2.2. Pravni okvir, ki se uporablja

Nacionalno pravo določa namenski pravni okvir, v skladu s katerim se vzpostavi podatkovna zbirka ter se opredelijo nameni obdelave in merila za vnos podatkov v podatkovno zbirko, dostop do nje in njeno uporabo. Zakonodajni ukrepi, potrebni za njegovo izvajanje, predvidevajo tudi določitev obdobja hrambe ter sklicevanje na veljavni načeli celovitosti in zaupnosti. Zakonodajni ukrepi predvidevajo tudi načine zagotavljanja informacij posamezniku, na katerega se nanašajo osebni podatki, in v tem primeru nosilcu(-em) starševske odgovornosti ter uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, in morebitno omejitev, če je ustrezno. Med pripravo predloga zadevnega zakonodajnega ukrepa se je bilo treba posvetovati z nacionalnim nadzornim organom.

2.3. Nujnost in sorazmernost – namen oziroma resnost kaznivega dejanja oziroma število oseb, ki niso vpletene, toda obdelava nanje vpliva

Pogoji in zaščitni ukrepi za obdelavo

Primerjavo na podlagi prepoznavanja obrazov lahko pooblaščeni uradnik opravi le kot zadnjo možnost, razen če niso na voljo druga manj vsiljiva sredstva in kadar je to nujno potrebno, na primer v primeru dvoma o verodostojnosti osebnega dokumenta mladoletnika, ki potuje, in/ali po pregledu predhodno zbranih dokazov in gradiva, ki kažejo na morebitno ujemanje z opisom pogrešanega otroka, v zvezi s katerim se izvaja kazenska preiskava.

Dodatna varovalka je zagotovljena tudi z obveznim pregledom in preverjanjem primerjave prepoznavanja obraza, kar izvede pooblaščeni uradnik, da se potrdijo predhodni dokazi z rezultatom primerjave in se izključijo morebitni lažno pozitivni rezultati.

Zasledovani cilj

Vzpostavitev podatkovne zbirke je namenjena izpolnjevanju pomembnih ciljev v splošnem javnem interesu, zlasti preprečevanju, preiskovanju, odkrivanju ali pregonu kaznivih dejanj ali izvrševanju kazenskih sankcij ter varstvu pravic in svoboščin drugih. Vzpostavitev podatkovne zbirke in predvidena obdelava naj bi pripomogli k identifikaciji otrok, ki so žrtve ugrabitve, zato se lahko štejeta za ukrep, primeren za podporo zakonitemu cilju preiskovanja in pregona takih kaznivih dejanj.

Namen in vnos podatkov v podatkovno zbirko

Nameni obdelave so jasno opredeljeni v zakonodaji in podatkovna zbirka se uporablja samo za identifikacijo pogrešanih otrok, za katere je bil prijavljen sum ugrabitve otroka, je bila uvedena kazenska preiskava pod nadzorom sodnega organa in je bil razpisan ukrep zaradi ugrabitve otroka. Cilj pogojev, ki jih zakonodaja določa za vnos podatkov v podatkovno zbirko, je strogo omejiti število posameznikov, na katere se nanašajo osebni podatki, in osebnih podatkov, ki jih je treba vključiti v podatkovno zbirko. Nosilec starševske odgovornosti za otroka mora biti obveščen o opravljeni obdelavi in pogojih za uveljavljanje otrokovih pravic v zvezi z biometrično obdelavo, predvideno za namen identifikacije, ali v zvezi z otrokovimi osebnimi podatki, shranjenimi v podatkovni zbirki.

2.4. Sklep

Ob upoštevanju nujnosti in sorazmernosti predvidene obdelave ter največje koristi otroka pri izvajanju take obdelave osebnih podatkov in pod pogojem, da so zagotovljena zadostna jamstva, ki zagotavljajo zlasti uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki – zlasti ob upoštevanju, da se bodo obdelovali podatki otrok –, se lahko šteje, da je taka uporaba obdelave s prepoznavanjem obraza verjetno združljiva s pravom EU.

Poleg tega EOVP glede na vrsto obdelave in uporabljeno tehnologijo, ki vključuje veliko tveganje za pravice in svoboščine zadevnega posameznika, na katerega se nanašajo osebni podatki, meni, da mora priprava predloga zakonodajnega ukrepa, ki naj bi ga sprejel nacionalni parlament, ali regulativnega ukrepa, ki temelji na takem zakonodajnem ukrepu, ki se nanaša na predvideno obdelavo, vključevati predhodno posvetovanje z nadzornim organom, da se zagotovita doslednost in skladnost s pravnim okvirom, ki se uporablja, prim. drugi odstavek 28. člena Direktive (EU) 2016/680.

3 SCENARIJ 3

3.1. Opis

Med policijskimi posredovanji v nemirih in preiskavami po njih so bile številne osebe prepoznane kot osumljenci, na primer v predhodnih preiskavah z uporabo posnetkov nadzornih kamer ali prič. Slike teh osumljencev se primerjajo s slikami oseb, ki so bile posnete z videonadzornimi sistemi CCTV ali mobilnimi napravami na kraju kaznivega dejanja ali v okolici.

Da bi policija pridobila podrobnejše dokaze o osebah, osumljenih sodelovanja v nemirih, ki so spremljali demonstracije, ustvari podatkovno zbirko, ki vsebuje slikovno gradivo, s približno lokalno in časovno povezavo z izgredi. Podatkovna zbirka vključuje zasebne posnetke, ki so jih policiji poslali državljani, gradivo iz videonadzornih sistemov CCTV v javnem prevozu, gradivo iz videonadzora, ki je v lasti policije, in gradivo, ki so ga brez posebnih omejitev ali varovalk objavili mediji. Prikaz hudega kaznivega ravnanja ni pogoj za zbiranje spisov v podatkovni zbirki. Zato so v podatkovni zbirki shranjeni tudi podatki oseb, ki niso sodelovale v nemirih – pomemben delež lokalnega prebivalstva, ki je med demonstracijami prišel mimo ali je sodeloval na demonstracijah, ne pa tudi v nemirih. Vsebuje več tisoč videoposnetkov in slikovnih datotek.

Z uporabo programske opreme za prepoznavanje obraza se vsem slikam obraza, ki se pojavijo v teh datotekah, dodelijo edinstvene identifikacijske oznake obraza. Slike obrazov posameznih osumljencev se nato samodejno primerjajo s temi osebnimi identifikacijskimi oznakami. Podatkovna zbirka, ki vsebuje vse biometrične predloge v več tisoč video- in slikovnih datotekah, se hrani do končanja vseh možnih preiskav. Pozitivne zadetke pregledajo odgovorni uradniki, ki se nato odločijo za nadaljnje ukrepe. To lahko vključuje dodelitev datoteke, najdene v zbirki podatkov, kazenski kartoteki zadevne osebe, in nadaljnje ukrepe, kot je zaslišanje ali prijetje zadevne osebe.

Nacionalna zakonodaja vsebuje splošno določbo, v skladu s katero je obdelava biometričnih podatkov za namene edinstvene identifikacije fizične osebe dopustna, če je to nujno potrebno in ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine zadevne osebe.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ vse osebe
- Vir slike: ☒ javno dostopna mesta ☒ zasebni subjekt ☒ drugi posamezniki ☒ drugo: mediji
- Povezava s kaznivim dejanjem: ☒ ne nujno neposredna geografska ali časovna povezava
- Način zajemanja informacij: ☒ na daljavo
- Okoliščine, ki vplivajo na druge temeljne pravice: Da, in sicer ☒ v okviru svobode zbiranja
- Možnosti za dodatne vire informacij o posamezniku, na katerega se nanašajo osebni podatki:
  ☒ drugo: ni izključeno (na primer uporaba bankomatov ali vstop v trgovine), saj na slikah ni mogoče razbrati motivov

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☒ specifične podatkovne zbirke, povezane s področjem kriminala

Algoritem:

- Vrsta obdelave: ☒ identifikacija s primerjanjem z več vzorci

Rezultat:

- Učinek: ☒ neposreden (na primer posameznik, na katerega se nanašajo osebni podatki, je lahko prijet ali zaslišan)
- Avtomatizirana odločitev: ☒ NE
- Trajanje hrambe podatkov: do zaključka vseh možnih preiskav

Pravna analiza:

- Vrsta predhodnega obvestila posamezniku, na katerega se nanašajo osebni podatki: ☒ na spletnem mestu organa kazenskega pregona na splošno
- Pravni okvir, ki se uporablja: ☒ Direktiva (EU) 2016/680 je bila večinoma kopirana v nacionalno pravo ☒ splošno nacionalno pravo, v skladu s katerim organi kazenskega pregona uporabljajo biometrične podatke

3.2. Pravni okvir, ki se uporablja

Kot je pojasnjeno zgoraj, pravne podlage, ki zgolj ponavljajo splošno določbo 10. člena Direktive (EU) 2016/680, niso dovolj jasne, da bi posameznikom ustrezno pojasnile pogoje in okoliščine, v katerih so organi kazenskega pregona pooblaščeni za uporabo posnetkov videonadzornih sistemov CCTV na javnih mestih za izdelavo biometrične predloge njihovega obraza in njeno primerjavo s policijskimi podatkovnimi zbirkami, drugimi razpoložljivimi posnetki videonadzornih sistemov CCTV ali zasebnimi posnetki itd. Pravni okvir, vzpostavljen v tem scenariju, zato ne izpolnjuje minimalnih zahtev, da bi se lahko uporabil kot pravna podlaga.

3.3. Nujnost in sorazmernost

V tem primeru obdelava vzbuja različne pomisleke v okviru načel nujnosti in sorazmernosti iz več razlogov:

Osebe niso osumljene hudega kaznivega dejanja. Prikaz hudega kaznivega ravnanja ni pogoj za uporabo datotek v podatkovni zbirki, ki vsebujejo slikovno gradivo. Tudi neposredna časovna in geografska povezava s kaznivim dejanjem nista pogoj za uporabo datotek v podatkovni zbirki. To pomeni, da so podatki velikega deleža lokalnega prebivalstva shranjeni v biometrični podatkovni zbirki za obdobje, ki lahko traja več let, dokler se vse preiskave ne končajo.

Podatkovna zbirka s podatki kraja kaznivega dejanja ni omejena na slike, ki izpolnjujejo zahteve glede sorazmernosti, kar vodi do neomejene količine slik, ki jih je treba primerjati. To je v nasprotju z načelom najmanjšega obsega podatkov. Manjše število slik bi omogočilo tudi uporabo nealgoritemskih in manj vsiljivih sredstev, na primer oseb z izjemnimi lastnostmi prepoznavanja podrobnosti[88].

Ker je primer vzet iz okolice protesta, je verjetno, da slike razkrivajo tudi politična stališča udeležencev demonstracij, kar je druga posebna vrsta podatkov, na katero bi se lahko vplivalo v tem scenariju. V tem scenariju ni jasno, kako je mogoče preprečiti zbiranje teh podatkov in s katerimi zaščitnimi ukrepi. Poleg tega lahko posamezniki, na katere se nanašajo osebni podatki, izvedo, da so bili zaradi sodelovanja na demonstracijah vpisani v policijsko zbirko biometričnih podatkov, kar ima lahko resne zastraševalne učinke v zvezi z njihovim prihodnjim uresničevanjem pravice do zbiranja.

Biometrične predloge v podatkovni zbirki je mogoče primerjati tudi med seboj. Tako lahko policija v svojem celotnem gradivu ne išče le specifične osebe, ampak tudi znova ustvari njen vedenjski vzorec v nekajdnevnem obdobju. Poleg tega lahko zbira dodatne informacije o osebah, kot so socialni stiki in politično udejstvovanje.

Poseganje še dodatno krepi dejstvo, da se podatki obdelujejo brez vednosti posameznikov, na katere se nanašajo osebni podatki.

Glede na to, da posamezniki ves čas snemajo fotografije in videoposnetke ter da je mogoče biometrično analizirati tudi gradivo vsepovsod prisotnih videonadzornih sistemov CCTV, lahko to povzroči resne zastraševalne učinke.

Še en razlog za zaskrbljenost je široka uporaba zasebnih fotografij in videoposnetkov, vključno z morebitno zlorabo, kot je kazenska ovadba. Ker je zloraba, kot je kazenska ovadba, tveganje, ki je neločljivo povezano tudi s kazenskimi postopki na splošno, je tveganje bistveno večje glede nadgradljivosti obdelanih podatkov in števila vpletenih oseb, saj lahko posamezniki naložijo tudi gradivo, ki se nanaša na specifično osebo ali skupino oseb, ki jim ni všeč. Pozivi policije v zvezi z nalaganjem fotografij in videoposnetkov lahko privedejo do zelo nizkih pragov, pri katerih bi ljudje lahko predložili gradivo, zlasti ker bi bilo to mogoče storiti anonimno ali vsaj brez potrebe, da bi se pojavili in se identificirali na policijski postaji.

3.4. Sklep

V tem primeru ni specifične določbe, ki bi se lahko uporabila kot pravna podlaga. Vendar tudi če bi bila zadostna pravna podlaga, zahtevi po nujnosti in sorazmernosti ne bi bili izpolnjeni, kar bi pomenilo

[88] To so ljudje z izjemno sposobnostjo prepoznavanja obrazov. Prim. tudi Face Recognition by Metropolitan Police Super-Recognisers, 26. februar 2016, DOI:10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

nesorazmeren poseg v pravice posameznika, na katerega se nanašajo osebni podatki, do spoštovanja zasebnega življenja in varstva osebnih podatkov v skladu z Listino.

4 SCENARIJ 4

4.1. Opis

Policija uvede način identifikacije osumljencev, ki so storili hudo kaznivo dejanje, posneto z videonadzornim sistemom CCTV, z naknadno obdelavo s tehnologijo za prepoznavanje obraza. Policist osebno izbere sliko(-e) osumljencev na videoposnetkih, ki so bili zbrani na kraju kaznivega dejanja ali drugje v okviru predhodne preiskave, in sliko(-e) nato pošlje forenzičnemu oddelku. Forenzični oddelek uporablja tehnologijo za prepoznavanje obraza in tako to (te) sliko(-e) primerja s slikami posameznikov, ki jih je policija predhodno zbrala v podatkovni zbirki (tako imenovana opisna podatkovna zbirka, ki vsebuje podatke osumljencev in nekdanjih obsojencev). Opisna podatkovna zbirka je za ta postopek – začasno in v izoliranem okolju – analizirana s tehnologijo za prepoznavanje obraza, da se lahko izvede postopek ujemanja. Da bi čim bolj zmanjšali poseganje v pravice in interese primerjanih oseb, ima dovoljenje za izvajanje dejanskega postopka ujemanja zelo malo zaposlenih v forenzičnem oddelku, dostop do podatkov je omejen na uradnike, ki jim je zaupana specifična zadeva, preden pa se rezultati pošljejo uradniku, ki vodi preiskavo, se rezultati še osebno pregledajo. Biometrični podatki se ne pošljejo ven iz nadzorovanega, izoliranega okolja. V preiskavi se dodatno uporabljata samo rezultat in slika (ne biometrična predloga). Zaposleni opravijo specifično usposabljanje o pravilih in postopkih za to obdelavo, vsa obdelava osebnih in biometričnih podatkov pa je zadostno podrobno opredeljena v nacionalnem pravu.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ osumljenci, identificirani na podlagi posnetkov videonadzornih sistemov CCTV
- Vir slike: ☒ javno dostopna mesta ☒ svetovni splet
- Povezava s kaznivim dejanjem: ☒ neposredna časovna povezava
  ☒ neposredna geografska povezava
- Način zajemanja informacij: ☒ na daljavo
- Okoliščine, ki vplivajo na druge temeljne pravice: Da, in sicer: ☒ svoboda zbiranja ☒ svoboda govora ☒ druge: __

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☒ specifične podatkovne zbirke, povezane s področjem kriminala

Algoritem:

- Vrsta obdelave: ☒ identifikacija s primerjanjem z več vzorci

Rezultat:

- Učinek: ☒ neposreden (na primer posameznik, na katerega se nanašajo osebni podatki, je prijet ali zaslišan)
- Avtomatizirana odločitev: ☒ NE

Pravna analiza:

- Pravni okvir, ki se uporablja: ☒ specifično nacionalno pravo za to obdelavo (prepoznavanje obraza) za zadevni pristojni organ

4.2. Pravni okvir, ki se uporablja

V tem scenariju je v nacionalnem pravu določeno, da se biometrični podatki lahko uporabijo pri izvajanju forenzične analize, kadar je to nujno potrebno, da se doseže namen identifikacije osumljencev, ki so storili hudo kaznivo dejanje, na podlagi ujemanja slik v opisni podatkovni zbirki. V nacionalnem pravu je določeno, kateri podatki se lahko obdelujejo, poleg tega so opredeljeni postopki za ohranjanje celovitosti in zaupnosti osebnih podatkov in postopki za njihovo uničenje, s čimer se zagotavljajo zadostna jamstva proti tveganju zlorabe in samovoljnemu ravnanju.

4.3. Nujnost in sorazmernost

Uporaba prepoznavanja obraza je očitno časovno učinkovitejša kot ujemanje, ki se na forenzični ravni ugotavlja osebno. Predhodno osebno izbiranje posnetkov omejuje poseganje v primerjavi s preverjanjem celotnega videogradiva v smislu ujemanja s podatki v podatkovni zbirki ter tako razlikuje in se ciljno usmerja samo na osebe, ki jih zajema cilj, tj. boj proti hudim kaznivim dejanjem. Pri tem pa je še vedno pomembno proučiti, ali je mogoče ujemanje, ki se izvaja osebno, opraviti v razumnem času, odvisno od obravnavanega primera. Omejitev števila oseb, ki imajo dostop do tehnologije in osebnih podatkov, zmanjšuje vpliv na pravico do zasebnosti in varstva podatkov, poleg tega se biometrične predloge ne shranjujejo ali uporabljajo pozneje v preiskavi. Osebni pregled rezultatov pomeni tudi manjše tveganje za lažno pozitivne rezultate.

4.4. Sklep

Pomembno je, da nacionalno pravo zagotavlja ustrezno pravno podlago za obdelavo biometričnih podatkov in za nacionalno podatkovno zbirko, s podatki katere se ugotavlja ujemanje. V tem scenariju so bili sprejeti številni ukrepi za omejitev poseganja v pravice do varstva podatkov, kot so pogoji za uporabo tehnologije za prepoznavanje obraza, podrobno opredeljeni v pravni podlagi, število ljudi, ki imajo dostop do tehnologije in biometričnih podatkov, osebni pregled rezultatov itd. Tehnologija za prepoznavanje obraza močno izboljša učinkovitost preiskovalnega dela forenzičnega oddelka policije, temelji na zakonu, ki policiji omogoča obdelavo biometričnih podatkov, kadar je to nujno potrebno, in se zato v okviru teh lastnosti lahko šteje za zakonito poseganje v pravice posameznika.

5 SCENARIJ 5

5.1. Opis

Za biometrično identifikacijo na daljavo gre, kadar se identiteta oseb ugotovi na podlagi biometričnih identifikatorjev (slike obraze, načina hoje, šarenice itd.) na daljavo, na javnem mestu ter na neprekinjen ali stalen način s preverjanjem na podlagi (biometričnih) podatkov, shranjenih v podatkovni zbirki[89]. Biometrična identifikacija na daljavo se izvaja v realnem času, če se snemanje slikovnega gradiva, primerjava in identifikacija zgodijo brez večjih časovnih razlik.

Pred vsako uvedbo biometrične identifikacije na daljavo v realnem času policija v okviru preiskave sestavi seznam nadzorovanih oseb, ki so predmet preiskave. Vsebuje slike obrazov posameznikov. Policija se na podlagi obveščevalnih podatkov, iz katerih je razvidno, da bodo posamezniki na specifičnem območju, na primer v nakupovalnem središču ali na javnem trgu, odloči, kdaj, kje in kako dolgo bo uporabljala biometrično identifikacijo na daljavo.

Na dan ukrepanja se na terenu postavi policijski kombi kot nadzorni center, v katerem je višji policijski uradnik. V tem kombiju so monitorji, na katerih se prikazujejo posnetki videonadzornih sistemov CCTV, nameščenih v bližini, pri čemer so kamere lahko bile nameščene priložnostno ali so se povezale z

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

videonadzornimi sistemi že nameščenih kamer. Ko gredo pešci mimo kamer, tehnologija izolira slike obraza, jih pretvori v biometrično predlogo in jih primerja z biometričnimi predlogami oseb s seznama nadzorovanih oseb.

Če se ugotovi potencialno ujemanje podatkov oseb na seznamu nadzorovanih oseb z osebami, ki gredo mimo kamer, sistem policiste v kombiju opozori na to ujemanje, ti policisti pa nato policistom na terenu sporočijo, da je opozorilo pozitivno, na primer po radijski povezavi. Policist na terenu se nato odloči, ali bo posredoval, se približal posamezniku ali ga nazadnje tudi prijel. Ukrepi, ki jih sprejme uradnik na terenu, so posneti. V primeru prikrite kontrole se shranjujejo zbrane informacije (na primer s kom je oseba, v kaj je oblečena in kam je namenjena).

Navedeno nacionalno pravo vsebuje splošno določbo, po kateri je obdelava biometričnih podatkov za namene edinstvene identifikacije fizične osebe dopustna, če je to nujno potrebno in ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine zadevne osebe.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ vse osebe
- Vir slike: ☒ javno dostopna mesta
- Povezava s kaznivim dejanjem: ☒ ne nujno neposredna geografska ali časovna povezava
- Način zajemanja informacij: ☒ na daljavo
- Okoliščine, ki vplivajo na druge temeljne pravice: Da, in sicer: ☒ svoboda zbiranja ☒ svoboda govora ☒ druge
- Možnosti za dodatne vire informacij o posamezniku, na katerega se nanašajo osebni podatki:
  ☒ drugo: ni izključeno (na primer uporaba bankomatov ali vstop v trgovine)

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☒ specifične podatkovne zbirke, povezane s področjem kriminala

Algoritem:

- Vrsta obdelave: ☒ identifikacija s primerjanjem z več vzorci

Rezultat:

- Učinek: ☒ neposreden (na primer posameznik, na katerega se nanašajo osebni podatki, je prijet ali zaslišan)
- Avtomatizirana odločitev: ☒ NE
- Trajanje hrambe podatkov: do zaključka vseh možnih preiskav

Pravna analiza:

- Vrsta predhodnega obvestila posamezniku, na katerega se nanašajo osebni podatki: ☒ na spletnem mestu organa kazenskega pregona na splošno
- Veljavni pravni okvir: ☒ Direktiva (EU) 2016/680 je bila večinoma kopirana v nacionalno pravo ☒ splošno nacionalno pravo, v skladu s katerim organi kazenskega pregona uporabljajo biometrične podatke

5.2. Pravni okvir, ki se uporablja

Pravne podlage, ki zgolj ponavljajo splošno določbo 10. člena Direktive (EU) 2016/680, niso dovolj jasne, da bi posameznikom ustrezno pojasnile pogoje in okoliščine, v katerih so organi kazenskega pregona pooblaščeni za uporabo posnetkov videonadzornih sistemov CCTV na javnih mestih za izdelavo biometrične predloge njihovega obraza in njeno primerjavo s policijskimi podatkovnimi

zbirkami. Pravni okvir, vzpostavljen v tem scenariju, zato ne izpolnjuje minimalnih zahtev, da bi se lahko uporabil kot pravna podlaga[90].

5.3. Nujnost in sorazmernost

Zahteva po nujnosti in sorazmernosti je tem večja, čim večji je poseg. Biometrična identifikacija na daljavo na javnih mestih ima številne posledice za temeljne pravice:

Scenariji vključujejo spremljanje vsakega mimoidočega na zadevnem javnem mestu. Tako močno vpliva na upravičeno pričakovanje prebivalstva glede anonimnosti na javnih mestih[91]. To je temeljni pogoj za številne vidike demokratičnega procesa, kot so odločitev za včlanitev v civilno združenje, obiskovanje zborovanj in srečevanje ljudi iz vseh družbenih in kulturnih okolij, sodelovanje na političnih protestih in obiskovanje raznovrstnih mest. Pojem anonimnosti na javnih mestih je ključen za prosto zbiranje in izmenjavo informacij ter idej. Ohranja pluralnost mnenj, svobodo mirnega zbiranja in združevanja ter varstvo manjšin in podpira načeli delitve oblasti ter sistema zavor in ravnovesij. Posledica spodkopavanja anonimnosti na javnih mestih lahko pomeni resen zastraševalni učinek na državljane. Lahko se vzdržijo nekaterih ravnanj, ki so nepogrešljiv del svobodne in odprte družbe. To bi vplivalo na javni interes, saj sta v demokratični družbi potrebna samoodločanje in sodelovanje njenih državljanov v demokratičnem procesu.

Če se taka tehnologija uporablja preprosto ob hoji po ulici, na poti do podzemne železnice ali do pekarne na prizadetem območju, bo to privedlo do tega, da bodo organi kazenskega pregona zbirali osebne podatke, vključno z biometričnimi podatki, in, v prvem scenariju, tudi do ujemanja s podatki v policijskih podatkovnih zbirkah. Položaj, v katerem bi isto storili z odvzemom prstnih odtisov, bi bil očitno nesorazmeren.

Število prizadetih posameznikov, na katere se nanašajo osebni podatki, je izjemno veliko, saj to vpliva na vse, ki se sprehodijo mimo zadevnega javnega mesta. Poleg tega bi scenariji pomenili avtomatizirano množično obdelavo biometričnih podatkov in množično ugotavljanje ujemanja biometričnih podatkov s podatki v policijskih podatkovnih zbirkah.

V evropski sodni praksi je množični nadzor prepovedan (na primer ESČP je v zadevi *S. in Marper proti Združenemu kraljestvu* menilo, da je neselektivna hramba biometričnih podatkov nesorazmeren poseg v pravico do zasebnosti, saj ga ni mogoče šteti za potrebnega v demokratični družbi).

Biometrična identifikacija na daljavo je tako nagnjena k množičnemu nadzoru, da ni zanesljivih sredstev za omejevanje. Bistveno se razlikuje od videonadzora kot takega, saj je možna uporaba videoposnetkov brez biometrične identifikacije že močan poseg, ki pa je hkrati omejen, v primeru uporabe tehnologije za prepoznavanje obraza pa se bo kakovost že razširjenega sistema videonadzora kot glavnega vira podatkov spremenila. Poleg tega, zlasti kar zadeva predvidene zastraševalne učinke, možne omejitve uporabe že nameščenih naprav za videonadzor ne bodo opazne, zato javnost temu ne bo zaupala.

Biometrična identifikacija na daljavo, ki jo opravijo policijski organi, vsakogar obravnava kot potencialnega osumljenca. V državi, ki deluje v skladu z načelom pravne države, pa se domneva, da so državljani nedolžni, dokler se kršitev ne dokaže. To načelo se delno izraža tudi v Direktivi

[90] V primerih, ko bi bilo treba v okviru znanstvenega projekta, namenjenega raziskovanju uporabe tehnologije za prepoznavanje obraza, obdelati osebne podatke, vendar taka obdelava ne bi spadala v področje uporabe tretjega odstavka 4. člena Direktive (EU) 2016/680 ali zunaj področja uporabe prava Unije, bi se uporabljala Splošna uredba o varstvu podatkov. V primeru pilotnih projektov, ki bi jim sledili ukrepi kazenskega pregona, bi se še vedno uporabljala Direktiva (EU) 2016/680.

[91] Odgovor EOVP poslancem Evropskega parlamenta v zvezi z aplikacijo za prepoznavanje obraza, ki jo je razvila družba Clearview AI, 10. junij 2020, ref.: OUT2020-0052.

(EU) 2016/680, ki poudarja, da je treba, kolikor je mogoče, razlikovati med obravnavo obsojencev ali osumljencev kaznivih dejanj, pri katerih morajo imeti organi kazenskega pregona „utemeljen sum, da so storile kaznivo dejanje ali ga nameravajo storiti“ (točka 6. člena Direktive (EU) 2016/680), in obravnavo tistih, ki niso obsojeni ali osumljeni kaznivih dejanj.

V prometnih vozliščih ali na javnih mestih bodo organi kazenskega pregona s tehnologijo, s katero bodo lahko edinstveno identificirali posameznika ter sledili in analizirali, kje se zadržuje in kje se giblje, razkrili vse najbolj občutljive informacije o posamezniku (celo spolno usmerjenost, veroizpoved in zdravstvene težave). S tem je povezano veliko tveganje nezakonitega dostopa do podatkov in njihove uporabe.

Namestitev sistema, ki omogoča odkrivanje jedra vedenja in značilnosti posameznika, vodi do močnih zastraševalnih učinkov. Zato se ljudje sprašujejo, ali naj se sploh pridružijo nekemu javnemu izražanju stališč, kar pa škoduje demokratičnemu procesu. Tudi srečanje z nekim prijateljem in to, da nekoga vidijo v javnosti s prijateljem, za katerega je znano, da ima težave s policijo ali da se obnaša na poseben način, se lahko šteje za nekaj kritičnega, saj bi vse to pritegnilo pozornost sistemskega algoritma in s tem organov kazenskega pregona.

Ranljivih posameznikov, na katere se nanašajo osebni podatki, kot so otroci, ni mogoče zaščititi. Poleg tega so s tem prizadete osebe, ki imajo poklicni interes – in pogosto ustrezno pravno obveznost –, da ohranjajo svoje stike zaupne, na primer novinarji, odvetniki in duhovniki. To bi lahko na primer vodilo do razkritja vira in novinarja ali dejstva, da se oseba posvetuje z zagovornikom. Težava ne velja le za naključna javna mesta, kjer se na primer srečujejo novinarji in njihovi viri, temveč seveda tudi za javna mesta, potrebna za pristop in dostop do ustanov ali strokovnjakov v zvezi s tem.

Poleg tega lahko nezadovoljstvo ljudi s tehnologijo za prepoznavanje obraza povzroči, da spremenijo svoje vedenje in se izogibajo krajem, kjer se uporablja ta tehnologija, ter se tako umaknejo od družbenega življenja in kulturnih prireditev. Glede na obseg uvedbe tehnologije za prepoznavanje obraza je lahko vpliv na ljudi tako velik, da vpliva na njihovo zmožnost za dostojno življenje[92].

Zato obstaja velika verjetnost, da bo to vplivalo na bistvo – nedotakljivo jedro – pravice do varstva osebnih podatkov. Močni znaki (prim. oddelek 3.1.3.2 smernic) so zlasti: organi kazenskega pregona v velikem obsegu avtomatizirano obdelujejo edinstvene biološke značilnosti ljudi, in to z algoritmi, ki temeljijo na verjetnosti, pri čemer je razlaga rezultatov le omejena. Omejitve pravic do zasebnosti in do varstva podatkov se uvedejo ne glede na posameznikovo ravnanje ali okoliščine, ki se nanašajo nanj. Statistično so skoraj vsi posamezniki, na katere se nanašajo osebni podatki in na katere vpliva to poseganje, dejansko posamezniki, ki spoštujejo zakonodajo. Možnosti za zagotavljanje informacij posamezniku, na katerega se nanašajo osebni podatki, so omejene. Sodno varstvo bo v večini primerov možno šele pozneje.

Zanašanje na sistem, ki temelji na verjetnosti in omejeni razložljivosti, lahko vodi do razpršene odgovornosti in pomanjkanja na področju pravnih sredstev ter je lahko spodbuda za malomarnost.

Ko se tak sistem, ki se lahko uporablja tudi za že nameščene kamere videonadzornih sistemov CCTV, uporabi, ga je mogoče z zelo majhnim naporom in ne da bi bil viden posameznikom, zlorabiti in omogočiti sistematično ter hitro pripravo seznamov ljudi glede na etnično poreklo, spol, vero itd.

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

Načelo obdelave osebnih podatkov na podlagi vnaprej določenih meril, na primer, kje se oseba zadržuje in po katerih poteh potuje, se že izvaja[93] in lahko se pojavi diskriminacija.

Glede na občutljivost, izraznost in količino obdelanih podatkov se sistemi za prepoznavanje obraza na daljavo na javno dostopnih mestih pogosto zlorabljajo s škodljivimi učinki za zadevne posameznike. Take podatke je mogoče zlahka zbrati in zlorabiti za izvajanje pritiska na ključne akterje v zvezi z načelom zavor in ravnovesij, kot so politična opozicija, uradniki in novinarji.

Nazadnje, sistemi za prepoznavanje obraza običajno vključujejo močne učinke pristranskosti glede rase in spola: lažno pozitivni rezultati nesorazmerno vplivajo na ljudi druge barve kože in ženske[94], kar povzroča diskriminacijo. Policijski ukrepi, ki sledijo lažno pozitivnim rezultatom, kot so preiskave in prijetja, te skupine še dodatno stigmatizirajo.

5.4. Sklep

Zgoraj navedeni scenariji v zvezi z obdelavo biometričnih podatkov na daljavo na javnih mestih za namene identifikacije ne vzpostavljajo pravičnega ravnotežja med nasprotujočimi si zasebnimi in javnimi interesi, kar pomeni nesorazmerno poseganje v pravice posameznika, na katerega se nanašajo osebni podatki, v skladu s 7. in 8. členom Listine.

6 SCENARIJ 6

6.1. Opis

Zasebni subjekt ponuja aplikacijo s podatkovno zbirko, v kateri so slike obraza, pobrane s svetovnega spleta. Uporabnik, na primer policija, lahko nato naloži sliko, aplikacija pa bo z uporabo biometrične identifikacije poskušala ugotoviti ujemanje s slikami obrazov ali biometričnimi predlogami v svoji podatkovni zbirki.

Lokalna policijska enota izvaja preiskavo kaznivega dejanja, za katero obstaja videoposnetek, pri čemer številnih potencialnih prič in osumljencev ni mogoče identificirati s primerjavo zbranih informacij z morebitnimi notranjimi podatkovnimi zbirkami ali obveščevalnimi podatki. Na podlagi zbranih informacij posamezniki niso registrirani v nobeni vzpostavljeni policijski podatkovni zbirki. Policija se odloči, da bo uporabila zgoraj omenjeno orodje, ki ga zagotavlja zasebno podjetje, da bi posameznike identificirala z biometrično identifikacijo.

Vir informacij:

- Vrste posameznikov, na katere se nanašajo osebni podatki: ☒ vsi državljani (priče) ☒ obsojenci ☒ osumljenci
- Vir slike: ☒ videoposnetek, pridobljen na javnem mestu ali drugje v okviru predhodne preiskave
- Povezava s kaznivim dejanjem: ☒ ni potrebna
- Način zajemanja informacij: ☒ na daljavo

[93] Prim. 6. člen Direktive (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj ter člen 33 Uredbe (EU) 2018/1240 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o vzpostavitvi Evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembi uredb (EU) št. 1077/2011, (EU) št. 515/2014, (EU) 2016/399, (EU) 2016/1624 in (EU) 2017/2226.

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

- Okoliščine, ki vplivajo na druge temeljne pravice: Da, in sicer: ☒ svoboda zbiranja ☒ svoboda govora ☒ druge: __

Referenčna podatkovna zbirka (s katero se primerjajo zbrane informacije):

- Specifičnost: ☒ podatkovne zbirke za splošne namene, ki vsebujejo podatke s svetovnega spleta

Algoritem:

- Vrsta obdelave: ☒ identifikacija s primerjanjem z več vzorci

Rezultat:

- Učinek: ☒ neposreden (npr. posameznik, na katerega se nanašajo osebni podatki, je prijet, zaslišan ali je zaznano diskriminatorno ravnanje)
- Avtomatizirana odločitev: ☒ NE

Pravna analiza:

- Vrsta predhodnega obvestila posamezniku, na katerega se nanašajo osebni podatki: ☒ Ne

6.2. Pravni okvir, ki se uporablja

Kadar zasebni subjekt zagotavlja storitev, ki vključuje obdelavo osebnih podatkov, za katero sam določi namen in sredstva (v tem primeru zbiranje slik s svetovnega spleta, da se ustvari podatkovna zbirka), mora imeti ta zasebni subjekt pravno podlago za to obdelavo. Poleg tega mora imeti organ kazenskega pregona, ki se odloči za uporabo te storitve za svoje namene, pravno podlago za obdelavo, za katero določi namene in sredstva. Da bi lahko organ kazenskega pregona obdeloval biometrične podatke, mora veljati pravni okvir, ki določa cilj. Ob tem je treba opredeliti osebne podatke, ki jih je treba obdelati, namene obdelave in postopke za ohranjanje celovitosti in zaupnosti osebnih podatkov ter postopke za njihovo uničenje.

Ta scenarij pomeni množično zbiranje osebnih podatkov od posameznikov, ki ne vedo, da se njihovi podatki zbirajo. Taka obdelava bi bila lahko zakonita le v zelo izjemnih okoliščinah. Glede na to, kje je zbirka podatkov shranjena, lahko uporaba take storitve pomeni prenos osebnih podatkov in/ali posebnih vrst osebnih podatkov ven iz Evropske unije (to lahko počne policija, kadar na primer pošilja sliko obraza v videoposnetku iz videonadzorne naprave ali drugače zbrane podatke), za to pa je treba izpolnjevati specifične pogoje za ta prenos, glej 39. člen Direktive (EU) 2016/680.

V tem scenariju ni specifičnih pravil, ki bi organu kazenskega pregona omogočala tako obdelavo.

6.3. Nujnost in sorazmernost

To, da storitev uporablja organ kazenskega pregona, pomeni, da se osebni podatki delijo z zasebnim subjektom, ki uporablja podatkovno zbirko, v kateri se osebni podatki zbirajo neomejeno in množično. Med zbranimi osebnimi podatki in ciljem, ki ga zasleduje organ kazenskega pregona, ni nikakršne povezave. Če organ kazenskega pregona podatke deli z zasebnim subjektom, to pomeni tudi, da organ nima nadzora nad podatki, ki jih obdeluje zasebni subjekt, posamezniki, na katere se nanašajo osebni podatki, pa imajo velike težave pri uresničevanju svojih pravic, saj ne vedo, da se njihovi podatki obdelujejo na ta način. To postavlja zelo visoko mejo za primere, v katerih bi se taka obdelava sploh lahko izvajala. Vprašljivo je, ali bi kateri koli cilj izpolnjeval zahteve iz omenjene direktive, saj se vsa odstopanja od pravic do zasebnosti in do varstva podatkov ter njihove omejitve uporabljajo le, kadar je to nujno potrebno. Splošni interes učinkovitosti v boju proti hudim kaznivim dejanjem sam po sebi ne more upravičiti obdelave, pri kateri se brez razlikovanja zbirajo tako velike količine podatkov. Ta obdelava zato ne bi izpolnjevala zahtev glede nujnosti in sorazmernosti.

6.4. Sklep

Zaradi pomanjkanja jasnih, natančnih in predvidljivih pravil, ki bi izpolnjevala zahteve iz 4. in 10. člena Direktive (EU) 2016/680, ter pomanjkanja dokazov, da je ta obdelava nujno potrebna, da se dosežejo postavljeni cilji, je mogoče sklepati, da uporaba te aplikacije ne bi izpolnjevala zahtev glede nujnosti in sorazmernosti ter bi pomenila nesorazmerno poseganje v pravici posameznikov, na katere se nanašajo osebni podatki, do spoštovanja zasebnega življenja in do varstva osebnih podatkov v skladu z Listino.