Gairės

Translations proofread by EDPB Members. This language version has not yet been proofread.

Gairės 05/2022 dėl veido atpažinimo technologijos naudojimo teisėsaugos srityje

Versija 2.0

Priimta 2023 m. balandžio 26 d.

Ankstesnės versijos

Versija 1.0	2022 m. gegužės 12 d.	Gairių priėmimas viešoms konsultacijoms
Versija 2.0	2023 m. balandžio 26 d.	Gairių priėmimas po viešų konsultacijų

Turinys

SANTRAUKA

Vis daugiau teisėsaugos institucijų taiko arba ketina taikyti veido atpažinimo technologiją. Ji gali būti naudojama asmeniui **atpažinti** arba jo **tapatybei nustatyti** ir gali būti taikoma vaizdo įrašams (pvz., AVSS) arba nuotraukoms. Ji gali būti naudojama įvairiais tikslais, be kita ko, siekiant ieškoti asmenų, įtrauktų į policijos stebėjimo sąrašus, arba stebėti asmens judėjimą viešojoje erdvėje.

Veido atpažinimo technologija grindžiama **biometrinių duomenų** tvarkymu, todėl ji apima specialių kategorijų asmens duomenų tvarkymą. Veido atpažinimo technologijoje neretai naudojami **dirbtinio intelekto** (DI) arba mašininio mokymosi komponentai. Nors tai sudaro sąlygas didelio masto duomenų tvarkymui, tai taip pat kelia diskriminacijos ir klaidingų rezultatų riziką. Veido atpažinimo technologija gali būti naudojama kontroliuojamose asmeninio kontakto situacijose, tačiau taip pat didžiulėse miniose ir dideliuose transporto mazguose.

Veido atpažinimo technologija teisėsaugos institucijoms yra **jautri priemonė**. Teisėsaugos institucijos yra vykdomosios valdžios institucijos, turinčios suverenių galių. Naudojant veido atpažinimo technologiją, tikėtina, kad gali būti varžomos pagrindinės teisės, be to, ne tik teisė į asmens duomenų apsaugą, ir tai gali daryti poveikį mūsų socialiniam ir demokratiniam politiniam stabilumui.

Kalbant apie asmens duomenų apsaugą teisėsaugos srityje, reikia laikytis **Teisėsaugos direktyvos reikalavimų**. Teisėsaugos direktyvoje nustatyta tam tikra veido atpažinimo technologijos naudojimo sistema, visų pirma Teisėsaugos direktyvos 3 straipsnio 13 punkte (terminas „biometriniai duomenys“), 4 straipsnyje (su asmens duomenų tvarkymu susiję principai), 8 straipsnyje (tvarkymo teisėtumas), 10 straipsnyje (specialių kategorijų asmens duomenų tvarkymas) ir 11 straipsnyje (automatizuotas individualių sprendimų priėmimas).

Veido atpažinimo technologijos taikymas taip pat gali daryti poveikį kelioms kitoms pagrindinėms teisėms. Todėl **ES pagrindinių teisių chartija** (toliau – Chartija) yra labai svarbi aiškinant Teisėsaugos direktyvą, visų pirma Chartijos 8 straipsnyje įtvirtinta teisė į asmens duomenų apsaugą, taip pat Chartijos 7 straipsnyje nustatyta teisė į privatų gyvenimą.

Teisėkūros priemonėmis, kurios yra asmens duomenų tvarkymo teisinis pagrindas, tiesiogiai varžomos Chartijos 7 ir 8 straipsniais garantuojamos teisės. Biometrinių duomenų tvarkymas bet kokiomis aplinkybėmis pats savaime yra didelis suvaržymas. Tai nepriklauso nuo rezultato, pvz., teigiamos atitikties. Bet koks šios pagrindinių teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės.

Teisinis pagrindas turi būti **pakankamai aiškus**, kad piliečiams būtų tinkamai nurodytos sąlygos ir aplinkybės, kuriomis valdžios institucijos yra įgaliotos imtis bet kokių duomenų rinkimo ir slapto sekimo priemonių. Vien perkėlus į nacionalinę teisę Teisėsaugos direktyvos 10 straipsnio bendrąją nuostatą, tikslumas ir nuspėjamumas nebūtų pakankami.

Prieš nacionaliniam teisės aktų leidėjui sukuriant naują teisinį pagrindą bet kokiam biometrinių duomenų tvarkymui naudojant veido atpažinimą, reikėtų **pasikonsultuoti** su kompetentinga duomenų apsaugos priežiūros institucija.

Teisėkūros priemonės turi būti **tinkamos** atitinkamais teisės aktais siekiamiems teisėtiems tikslams įgyvendinti. **Bendrojo intereso tikslas**, kad ir koks esminis jis būtų, pats savaime nepateisina pagrindinės teisės apribojimo. Teisėkūros priemonės turėtų būti **diferencijuojamos** ir taikomos asmenims, kuriems jos skirtos atsižvelgiant į tikslą, pvz., kovoti su konkrečiais sunkiais nusikaltimais. Jei priemonė taikoma visiems asmenims bendrai, be tokio diferencijavimo, apribojimo ar išimties,

suvaržymas tampa dar didesnis. Suvaržymas taip pat suintensyvėja, jei duomenų tvarkymas apima didelę gyventojų dalį.

Duomenys turi būti tvarkomi taip, kad būtų užtikrintas ES duomenų apsaugos taisyklių ir principų taikymas ir veiksmingumas. Atsižvelgiant į kiekvieną situaciją, **būtinumo ir proporcingumo vertinime** taip pat turi būti nustatytas ir apsvarstytas galimas poveikis kitoms pagrindinėms teisėms. Jei duomenys sistemingai tvarkomi be duomenų subjektų žinios, tikėtina, kad tai gali sukelti **bendrą nuolatinio stebėjimo jausmą**. Tai gali turėti atgrasomąjį poveikį, susijusį su kai kuriomis arba visomis atitinkamomis pagrindinėmis teisėmis, pavyzdžiui, žmogaus orumu pagal Chartijos 1 straipsnį, minties, sąžinės ir religijos laisve pagal Chartijos 10 straipsnį, saviraiškos laisve pagal Chartijos 11 straipsnį ir susirinkimų ir asociacijų laisve pagal Chartijos 12 straipsnį.

Specialių kategorijų duomenų, pavyzdžiui, biometrinių duomenų, tvarkymas gali būti laikomas „**tikrai būtinu**“ (Teisėsaugos direktyvos 10 straipsnis) tik tuo atveju, jei asmens duomenų apsaugos suvaržymas ir jo apribojimai apsiriboja tik tuo, kas yra absoliučiai būtina, t. y. neišvengiama, ir išskyrus bet kokį bendro ar sistemingo pobūdžio tvarkymą.

Tai, kad duomenų subjektas **akivaizdžiai viešai** paskelbė nuotrauką (Teisėsaugos direktyvos 10 straipsnis), nereiškia, kad susiję biometriniai duomenys, kuriuos galima gauti iš nuotraukos tam tikromis techninėmis priemonėmis, laikomi akivaizdžiai paskelbtais viešai. Standartinių paslaugos nustatymų, pvz., šablonų viešinimo, arba pasirinkimo nebuvimo, pvz., kai šablonai skelbiami viešai naudotojui negalint šio nustatymo pasirinkti, jokiu būdu negalima laikyti akivaizdžiai viešai paskelbtais duomenimis.

Teisėsaugos direktyvos 11 straipsnyje nustatyta **automatizuoto individualių sprendimų priėmimo** sistema. Veido atpažinimo technologijos naudojimas apima specialių kategorijų duomenų naudojimą ir gali lemti profiliavimą, priklausomai nuo to, kaip ir kokiu tikslu taikoma veido atpažinimo technologija. Bet kuriuo atveju pagal Sąjungos teisę ir Teisėsaugos direktyvos 11 straipsnio 3 dalį profiliavimas, sukeliantis fizinių asmenų diskriminaciją remiantis specialių kategorijų asmens duomenimis, draudžiamas.

Teisėsaugos direktyvos 6 straipsnyje kalbama apie būtinybę **atskirti skirtingų kategorijų duomenų subjektus**. Duomenų subjektų, kurių atžvilgiu nėra jokių įrodymų, leidžiančių manyti, kad jų elgesys gali būti susijęs, net ir netiesiogiai ar nedaug, su teisėtu tikslu pagal Teisėsaugos direktyvą, atžvilgiu suvaržymas greičiausiai nėra pateisinamas.

Pagal **duomenų kiekio mažinimo principą** (Teisėsaugos direktyvos 4 straipsnio 1 dalies e punktas) taip pat reikalaujama, kad bet kokia vaizdo medžiaga, nesusijusi su duomenų tvarkymo tikslu, visada būtų pašalinta arba nuasmeninta (pvz., užtušuojant, kad būtų neįmanoma atkurti duomenis) prieš ją panaudojant.

Prieš pradėdamas tvarkyti duomenis naudojant veido atpažinimo technologiją, duomenų valdytojas turi atidžiai apsvarstyti, kaip (arba ar jis gali) įvykdyti **duomenų subjekto teisių** reikalavimus, nes veido atpažinimo technologija dažnai apima specialių kategorijų asmens duomenų tvarkymą nesant jokio akivaizdaus bendravimo su duomenų subjektu.

Veiksmingas naudojimasis duomenų subjekto teisėmis priklauso nuo to, ar duomenų valdytojas įvykdys savo **informavimo pareigas** (Teisėsaugos direktyvos 13 straipsnis). Vertinant, ar tai „konkretus atvejis“ pagal Teisėsaugos direktyvos 13 straipsnio 2 dalį, reikia atsižvelgti į kelis veiksnius, įskaitant klausimą, ar asmens duomenys renkami be duomenų subjekto žinios, nes tai būtų vienintelis būdas sudaryti sąlygas duomenų subjektams veiksmingai naudotis savo teisėmis. Jei sprendimai priimami

remiantis tik veido atpažinimo technologija, duomenų subjektai turi būti informuojami apie automatizuoto sprendimų priėmimo charakteristikas.

Kalbant apie **prašymus leisti susipažinti su duomenimis**, kai biometriniai duomenys saugomi ir su tapatybe susieti ir raidiniais skaitmeniniais duomenimis, laikantis duomenų kiekio mažinimo principo, tai turėtų leisti kompetentingai institucijai patvirtinti prašymą leisti susipažinti su duomenimis atlikus paiešką pagal šiuos raidinius skaitmeninius duomenis ir nepradedant jokio tolesnio kitų asmenų biometrinių duomenų tvarkymo (t. y. atliekant paiešką duomenų bazėje naudojant veido atpažinimo technologiją).

Pavojus duomenų subjektams yra ypač rimtas, jeigu policijos duomenų bazėje saugomi netikslūs duomenys ir (arba) jais dalijamasi su kitais subjektais. Duomenų valdytojas turi atitinkamai **ištaisyti** saugomus duomenis ir veido atpažinimo technologijos sistemas (taip pat žr. Teisėsaugos direktyvos 47 konstatuojamąją dalį).

Teisė **apriboti duomenų tvarkymą** tampa ypač svarbi, kai veido atpažinimo technologija (grindžiama algoritmu (-ais) ir todėl niekada nerodanti galutinio rezultato) taikoma tais atvejais, kai renkami dideli duomenų kiekiai ir tapatybės nustatymo tikslumas bei kokybė gali skirtis.

Poveikio duomenų apsaugai vertinimas (PDAV) prieš naudojant veido atpažinimo technologiją yra privalomas reikalavimas, plg. Teisėsaugos direktyvos 27 straipsnį. Kaip pasitikėjimo ir skaidrumo didinimo priemonę, EDAV rekomenduoja viešai skelbti tokių vertinimų rezultatus arba bent pagrindinius duomenų apsaugos poveikio vertinimo (PDAV) nustatytus faktus ir išvadas.

Dauguma veido atpažinimo technologijos diegimo ir naudojimo atvejų duomenų subjektų teisėms ir laisvėms iš esmės kelia didelę riziką. Todėl veido atpažinimo technologiją taikanti institucija prieš įdiegdama šią sistemą turėtų **pasikonsultuoti** su kompetentinga priežiūros institucija.

Atsižvelgiant į unikalų biometrinių duomenų pobūdį, veido atpažinimo technologiją įdiegusi ir (arba) naudojanti institucija turėtų skirti ypatingą dėmesį **duomenų tvarkymo saugumui**, kaip nustatyta Teisėsaugos direktyvos 29 straipsnyje. Visų pirma teisėsaugos institucija turėtų užtikrinti, kad sistema atitiktų atitinkamus standartus ir kad joje būtų įdiegtos biometrinių duomenų šablonų apsaugos priemonės. Duomenų apsaugos principai ir apsaugos priemonės turi būti integruoti į technologiją prieš pradedant tvarkyti asmens duomenis. Todėl net ir tais atvejais, kai teisėsaugos institucija ketina taikyti ir naudoti išorės paslaugų teikėjų veido atpažinimo technologiją, ji turi užtikrinti, pavyzdžiui, surengdama viešųjų pirkimų procedūrą, kad būtų naudojama tik **integruotosios ir standartizuotosios duomenų apsaugos** principais pagrįsta veido atpažinimo technologija.

Registravimas (plg. Teisėsaugos direktyvos 25 straipsnį) yra svarbi apsaugos priemonė, siekiant patikrinti duomenų tvarkymo teisėtumą tiek vidaus lygmeniu (t. y. atitinkamo duomenų valdytojo (tvarkytojo) vykdoma savikontrolė), tiek išorės priežiūros institucijų lygmeniu. Veido atpažinimo sistemose rekomenduojama registruoti ir etaloninės duomenų bazės pakeitimus bei tapatybės nustatymo ar tikrinimo bandymus, įskaitant naudotoją, rezultatą ir patikimumo įvertinimą. Tačiau registravimas yra tik vienas iš esminių bendro **atskaitomybės principo** elementų (plg. Teisėsaugos direktyvos 4 straipsnio 4 dalį). Duomenų valdytojas turi galėti įrodyti, kad duomenų tvarkymas atitinka Teisėsaugos direktyvos 4 straipsnio 1–3 dalyse nustatytus pagrindinius duomenų apsaugos principus.

EDAV primena savo ir EDAPP bendrą **raginimą uždrausti** tam tikrų rūšių duomenų tvarkymą, susijusį su 1) nuotoliniu biometriniu asmenų tapatybės nustatymu viešosiose erdvėse, 2) DI grindžiamo veido atpažinimo sistemomis, kurias naudojant asmenys pagal jų biometrinius duomenis skirstomi į grupes pagal etninę kilmę, lytį, taip pat politinę ar seksualinę orientaciją ar kitus diskriminacijos pagrindus, 3)

veido atpažinimo ar panašių technologijų naudojimu siekiant nustatyti fizinio asmens emocijas ir 4) asmens duomenų tvarkymu teisėsaugos srityje naudojant duomenų bazę, pildomą masiškai ir nesirenkamai kaupiant asmens duomenis, pvz., perimant internete prieinamas nuotraukas ir veido atvaizdus.

Labai svarbi nagrinėjamų pagrindinių teisių apsaugos priemonė yra kompetentingų duomenų apsaugos priežiūros institucijų vykdoma **veiksminga priežiūra**. Todėl valstybės narės turi užtikrinti, kad priežiūros institucijų ištekliai būtų tinkami ir pakankami, kad jos galėtų vykdyti savo įgaliojimus.

Šios **gairės skirtos** ES ir nacionalinio lygmens teisės aktų leidėjams, teisėsaugos institucijoms ir jų pareigūnams, įgyvendinantiems ir naudojantiems veido atpažinimo technologijos sistemas. Jos skirtos asmenims tiek, kiek jie suinteresuoti apskritai arba kaip duomenų subjektai, visų pirma kiek tai susiję su duomenų subjektų teisėmis.

Gairėmis ketinama informuoti apie tam tikras veido atpažinimo technologijos savybes ir teisėsaugos srityje taikytiną teisinę sistemą (visų pirma Teisėsaugos direktyvą).

- Be to, jose pateikiama **įrankių, padedančių pirmą kartą nustatyti konkretaus naudojimo atvejo jautrumą** (I priedas).
- Jose taip pat pateikiamos **praktinės rekomendacijos teisėsaugos institucijoms, norinčioms įsigyti ir naudoti veido atpažinimo technologijos sistemą** (II priedas).
- Gairėse taip pat aprašyti keli tipiniai **naudojimo atvejai ir pateikta daug svarbių įžvalgų**, ypač susijusių su būtinumo ir proporcingumo patikra (III priedas).

1 ĮVADAS

1. Veido atpažinimo technologija gali būti naudojama siekiant automatiškai atpažinti asmenis pagal jų veidą. Veido atpažinimo technologija neretai grindžiama dirbtiniu intelektu, pavyzdžiui, mašininio mokymosi technologijomis. Veido atpažinimo technologijos taikomosios programos vis dažniau išbandomos ir naudojamos įvairiose srityse – nuo individualaus naudojimo iki naudojimo privačiose organizacijose ir viešojo administravimo įstaigose. Naudos iš veido atpažinimo technologijos naudojimo tikisi ir teisėsaugos institucijos. Ši technologija žada sprendimus, susijusius su palyginti naujais iššūkiais, pavyzdžiui, tyrimais, susijusiais su dideliu kiekiu surinktų įrodymų, taip pat su žinomomis problemomis, visų pirma susijusiomis su nepakankamu darbuotojų skaičiumi stebėjimo ir paieškos užduotims atlikti.

2. Susidomėjimas veido atpažinimo technologija padidėjo daugiausia dėl jos veiksmingumo ir išplečiamumo. Dėl šių savybių atsiranda ir trūkumų, susijusių su šia technologija ir jos taikymu; tie trūkumai taip pat gali būti didelio masto. Nors vienu mygtuko paspaudimu gali būti išanalizuoti tūkstančiai asmens duomenų rinkinių, dėl net nedidelio algoritmo lemiamos diskriminacijos ar neteisingo tapatybės nustatymo poveikio daugelio žmonių elgesys ir kasdienis gyvenimas gali būti smarkiai paveiktas. Asmens duomenų, visų pirma biometrinių duomenų, tvarkymo mastas pats savaime yra dar vienas svarbus veido atpažinimo technologijos elementas, nes asmens duomenų tvarkymas yra pagrindinės teisės į asmens duomenų apsaugą pagal Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 8 straipsnį suvaržymas.

3. Veido atpažinimo technologijos taikymas teisėsaugos institucijose turės – ir tam tikru mastu jau turi – reikšmingų pasekmių asmenims ir asmenų grupėms, įskaitant mažumas. Tos pasekmės taip pat turės didelį poveikį mūsų sambūviui ir mūsų socialiniam bei demokratiniam politiniam stabilumui, vertybe

laikant didelę pliuralizmo ir politinės opozicijos svarbą. Teisė į asmens duomenų apsaugą neretai yra būtina sąlyga siekiant užtikrinti kitas pagrindines teises. Taikant veido atpažinimo technologiją labai tikėtina, kad gali būti varžomos pagrindinės teisės, ne tik teisė asmens duomenų apsaugą.

4. Todėl EDAV mano, kad svarbu prisidėti prie tebevykstančios veido atpažinimo technologijos integracijos teisėsaugos srityje, kuriai taikoma Teisėsaugos direktyva[1], atitinkamai nacionalinės teisės aktai, kuriais ji perkeliama į nacionalinę teisę, ir pateikti šias gaires. Gairėmis siekiama teikti aktualią informaciją ES ir nacionalinio lygmens teisės aktų leidėjams, taip pat teisėsaugos institucijoms ir jų pareigūnams įgyvendinant ir naudojant veido atpažinimo technologijos sistemas. Gairių taikymo sritį sudaro tik veido atpažinimo technologija. Tačiau kitų formų teisėsaugos institucijų vykdomas asmens duomenų tvarkymas remiantis biometriniais duomenimis, ypač jei jis vyksta nuotoliniu būdu, gali kelti panašų arba papildomą pavojų asmenims, grupėms ir visuomenei. Atsižvelgiant į atitinkamas aplinkybes, kai kurie šių gairių aspektai gali būti naudingas šaltinis ir tokiais atvejais. Galiausiai asmenys, kurie yra suinteresuoti apskritai arba kaip duomenų subjektai, taip pat gali rasti svarbios informacijos, visų pirma susijusios su duomenų subjektų teisėmis.

5. Gaires sudaro pagrindinė dalis ir trys priedai. Pagrindinėje dalyje pristatoma technologija ir taikytina teisinė sistema. Siekiant padėti nustatyti kai kuriuos svarbiausius aspektus, kad būtų galima įvertinti pagrindinių teisių apribojimo tam tikroje taikymo srityje sunkumą, I priede pateikiamas šablonas. Teisėsaugos institucijos, norinčios įsigyti ir naudoti veido atpažinimo technologiją, praktinių rekomendacijų gali rasti II priede. Atsižvelgiant į veido atpažinimo technologijos taikymo sritį, gali būti svarbūs įvairūs aspektai. III priede pateikiamas hipotetinių scenarijų ir svarbių aplinkybių rinkinys.

2 TECHNOLOGIJA

2.1 Viena biometrinė technologija, dvi skirtingos funkcijos

6. Veido atpažinimas – tai tikimybinė technologija, kuria galima automatiškai atpažinti asmenis pagal jų veidą, kad būtų galima patvirtinti arba nustatyti jų tapatybę.

7. Veido atpažinimo technologija priklauso platesnei biometrinių technologijų kategorijai. Biometrinės technologijos apima visus automatizuotus procesus, naudojamus asmeniui atpažinti pagal fizines, fiziologines ar elgsenos savybes (pirštų atspaudus, rainelės struktūrą, balsą, eiseną, kraujagyslių raštus ir kt.). Šios savybės apibrėžiamos kaip „biometriniai duomenys“, nes jos leidžia nustatyti arba patvirtinti unikalią asmens tapatybę.

8. Tai žmonių veidai arba, tiksliau, jų techninis apdorojimas naudojant veido atpažinimo prietaisus: padarant veido atvaizdą (nuotrauką arba vaizdo įrašą), vadinamą biometrinių duomenų pavyzdžiu, galima išgauti skaitmeninį šio veido skiriamųjų bruožų atvaizdą (tai vadinama šablonu).

9. Biometrinių duomenų šablonas – tai unikalių savybių, kurios buvo paimtos iš biometrinių duomenų pavyzdžio ir gali būti saugomos biometrinių duomenų bazėje, skaitmeninis atvaizdas[2]. Šis šablonas turi būti unikalus ir būdingas konkrečiam asmeniui ir iš esmės laikui bėgant išlieka nuolatinis[3]. Atpažinimo etape prietaisas šį šabloną lygina su kitais šablonais, sukurtais arba apskaičiuotais tiesiogiai remiantis

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.

[2] Veido atpažinimo gairės, 108-osios konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu konsultacinis komitetas, Europos Taryba, 2021 m. birželio mėn.

[3] Tai gali priklausyti nuo biometrinių duomenų rūšies ir duomenų subjekto amžiaus.

biometrinių duomenų pavyzdžiais, kaip antai paveikslėlyje, nuotraukoje ar vaizdo įraše esančiais veidais. Taigi „veido atpažinimas“ yra dviejų etapų procesas: veido atvaizdo duomenų surinkimas ir jo transformavimas į šabloną, po to šio veido atpažinimas lyginant atitinkamą šabloną su vienu ar keliais kitais šablonais.

10. Kaip ir bet kuris biometrinis procesas, veido atpažinimas gali atlikti dvi atskiras funkcijas:

- asmens **tapatybės patvirtinimo**, kai siekiama patikrinti, ar asmuo yra tas, kas teigia esąs. Tokiu atveju sistema lygins anksčiau užregistruotą biometrinių duomenų šabloną ar pavyzdį (pvz., saugomą lustinėje kortelėje arba biometriniame pase) su vienu veidu, pavyzdžiui, į patikrinimo punktą atvykusio asmens veidu, siekiant patikrinti, ar tai tas pats asmuo. Taigi ši funkcija grindžiama dviejų šablonų palyginimu. Tai taip pat vadinama **patikrinimu** „1 su 1“;
- asmens **tapatybės nustatymo**, kai siekiama surasti asmenį asmenų grupėje, tam tikroje teritorijoje, atvaizde ar duomenų bazėje. Šiuo atveju sistema turi apdoroti kiekvieną užfiksuotą veidą, sukurti biometrinių duomenų šabloną ir tada patikrinti, ar jis atitinka kurį nors sistemai žinomą asmenį. Taigi ši funkcija grindžiama vieno šablono palyginimu su šablonų arba pavyzdžių duomenų baze (baziniu lygiu). Tai taip pat vadinama tapatybės nustatymu lyginant „1 su daugeliu“. Pavyzdžiui, taip galima susieti asmenvardžio įrašą (pavardę, vardą) su veidu, jei palyginimas daromas nuotraukų, susietų su pavardėmis ir vardais, duomenų bazėje. Tokiu būdu asmuo taip pat gali būti sekamas minioje, nebūtinai susiejant jį su jo civiline tapatybe.

11. Abiem atvejais naudojami veido atpažinimo metodai yra pagrįsti apskaičiuotąja šablonų atitiktimi: lyginamo šablono ir bazinio (-ių) lygio (-ių). Šiuo požiūriu jie yra tikimybiniai: lyginant išvedama didesnė ar mažesnė tikimybė, kad asmuo iš tikrųjų yra asmuo, kurio tapatybė turi būti patvirtinta arba nustatyta; jeigu ši tikimybė viršija tam tikrą sistemoje nustatytą ribinę vertę, kurią apibrėžia sistemos naudotojas arba kūrėjas, sistema darys prielaidą, kad yra atitiktis.

12. Nors šios dvi funkcijos – tapatybės patvirtinimo ir tapatybės nustatymo – yra skirtingos, jos abi yra susijusios su biometrinių duomenų, susietų su identifikuotu arba identifikuojamu fiziniu asmeniu, tvarkymu, todėl tai yra asmens duomenų tvarkymas, tiksliau, specialių kategorijų asmens duomenų tvarkymas.

13. Veido atpažinimas yra dalis platesnio vaizdo apdorojimo metodų spektro. Kai kuriomis vaizdo kameromis galima filmuoti žmones tam tikroje teritorijoje, visų pirma jų veidus, tačiau jos negali būti naudojamos asmenims automatiškai atpažinti. Tas pats pasakytina ir apie paprastą fotografiją: kamera nėra veido atpažinimo sistema, nes norint gauti biometrinių duomenų žmonių nuotraukas reikia specialiu būdu apdoroti.

14. Vien tik veidų aptikimas vadinamosiomis „išmaniosiomis“ kameromis taip pat nebūtinai yra veido atpažinimo sistema. Nors dėl jų taip pat kyla svarbių etikos ir veiksmingumo klausimų, skaitmeniniai metodai, skirti neįprastam elgesiui ar smurtiniams įvykiams aptikti arba veido emocijoms ar net siluetams atpažinti, negali būti laikomi biometrinių duomenų sistemomis, kuriose tvarkomi specialių kategorijų asmens duomenys, jeigu jais nesiekiama nustatyti konkretaus asmens tapatybę ir jeigu tvarkomi asmens duomenys neapima kitų specialių kategorijų asmens duomenų. Šie pavyzdžiai nėra visiškai nesusiję su veido atpažinimu ir jiems vis tiek taikomos asmens duomenų apsaugos taisyklės[4].

[4] Tačiau Teisėsaugos direktyvos 10 straipsnis (arba BDAR 9 straipsnis) taikomas sistemoms, kurios naudojamos norint suskirstyti asmenis pagal jų biometrinius duomenis į grupes pagal etninę kilmę, politinę ar seksualinę orientaciją arba kitų specialių kategorijų asmens duomenis.

Be to, šios rūšies aptikimo sistema gali būti naudojama kartu su kitomis sistemomis, kuriomis siekiama nustatyti asmens tapatybę, todėl ji gali būti laikoma veido atpažinimo technologija.

15. Kitaip nei, pavyzdžiui, vaizdo įrašymo ir apdorojimo sistemose, kurioms reikia įrengti fizinius prietaisus, veido atpažinimas yra programinės įrangos funkcija, kurią galima įdiegti esamose sistemose (kamerose, vaizdų duomenų bazėse ir kt.). Todėl tokios funkcijos gali būti sujungtos ar susietos su daugybe sistemų ir naudojamos kartu su kitomis funkcijomis. Tokiam integravimui į jau esamą infrastruktūrą reikia skirti ypatingą dėmesį, nes jis susijęs su neišvengiama rizika dėl to, kad veido atpažinimo technologija gali būti nepastebima ir ją lengva paslėpti[5].

2.2 Įvairios paskirtys ir pritaikymo sritys

16. Neatsižvelgiant į šių gairių taikymo sritį ir į Teisėsaugos direktyvos taikymo sritį, veido atpažinimas gali būti naudojamas siekiant įvairių tikslų – tiek komercinių, tiek susijusių su visuomenės saugumo ar teisėsaugos klausimais. Ši technologija gali būti taikoma įvairiomis aplinkybėmis: naudotojui užmezgant asmeninį ryšį su paslauga (prieiga prie taikomosios programos), siekiant patekti į tam tikrą vietą (fizinis filtravimas) arba be jokių konkrečių apribojimų viešojoje erdvėje (veido atpažinimas tikruoju laiku). Ji gali būti taikoma bet kokios rūšies duomenų subjektams: paslaugos klientui, darbuotojui, paprastam praeiviui, ieškomam asmeniui arba asmeniui, dalyvaujančiam teisiniame ar administraciniame procese, ir kt. Kai kurie naudojimo būdai jau yra įprasti ir plačiai paplitę; su kitais šiuo metu eksperimentuojama arba dėl jų diskutuojama. Nors šiose gairėse nebus nagrinėjami visi tokie naudojimo ir taikymo būdai, EDAV primena, kad jie gali būti įgyvendinami tik tuo atveju, jei atitinka taikytiną teisinę sistemą, visų pirma BDAR ir atitinkamus nacionalinės teisės aktus[6]. Net ir Teisėsaugos direktyvos atveju, be tapatybės patvirtinimo arba tapatybės nustatymo funkcijų, duomenys, tvarkomi naudojant veido atpažinimo technologiją, taip pat gali būti toliau tvarkomi kitais tikslais, pavyzdžiui, siekiant suskirstyti į kategorijas.

17. Konkrečiau, galimų naudojimo būdų mastas galėtų būti vertinamas atsižvelgiant į tai, kiek asmenys kontroliuoja savo asmens duomenis, veiksmingas priemones, kurias jie turi tokiai kontrolei vykdyti, ir jų teisę imtis iniciatyvos aktyvuoti ir naudoti šią technologiją, pasekmes jiems (atpažinimo arba neatpažinimo atveju) ir atliekamo duomenų tvarkymo mastą. Veido atpažinimas pagal šabloną, saugomą tam asmeniui priklausančiame asmeniniame įrenginyje (lustinėje kortelėje, išmaniajame telefone ir kt.), naudojamame tapatybei patvirtinti ir skirtame naudoti tik asmeniniais tikslais per specialią sąsają, nekelia tokios pat rizikos kaip, pavyzdžiui, naudojimas tapatybės nustatymo tikslais nekontroliuojamoje aplinkoje, duomenų subjektams aktyviai nedalyvaujant, kai kiekvieno į stebėjimo zoną patenkančio veido šablonas lyginamas su duomenų bazėje saugomais didelės gyventojų grupės šablonais. Tarp šių dviejų kraštutinumų yra labai plataus spektro įvairių naudojimo būdų ir dėl jų kylančių klausimų, susijusių su asmens duomenų apsauga.

18. EDAV mano, kad siekiant išsamiau paaiškinti aplinkybes, kuriomis šiuo metu svarstomos ar diegiamos veido atpažinimo technologijos, skirtos tapatybei patvirtinti arba nustatyti, svarbu paminėti keletą pavyzdžių. Toliau pateikti pavyzdžiai yra tik aprašomojo pobūdžio ir neturėtų būti laikomi kokiu nors išankstiniu jų atitikties ES *acquis* duomenų apsaugos srityje vertinimu.

Veido atpažinimo technologijos naudojimo tapatybei patvirtinti pavyzdžiai

19. Tapatybės patvirtinimas gali būti vykdomas taip, kad naudotojai galėtų jį visiškai kontroliuoti, pavyzdžiui, kad būtų galima naudotis paslaugomis ar taikomosiomis programomis tiesiog namų

[5] Pavyzdžiui, ant kūno nešiojamose kamerose, kurios vis dažniau naudojamos praktikoje.
[6] Taip pat žr. 2020 m. sausio 29 d. priimtas EDPB gaires 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus, kuriose pateikiama papildomų rekomendacijų.

aplinkoje. Todėl šia technologija plačiai naudojasi išmaniųjų telefonų turėtojai, kad atrakintų savo įrenginį, užuot patvirtindami savo tapatybę slaptažodžiu.

20. Veido atpažinimo technologija tapatybei patvirtinti taip pat gali būti naudojama tikrinant asmens, kuris nori pasinaudoti viešosiomis ar privačiosiomis trečiųjų šalių paslaugomis, tapatybę. Taigi tokie procesai suteikia galimybę susikurti skaitmeninę tapatybę naudojantis mobiliąja programėle (išmaniuoju telefonu, planšetiniu kompiuteriu ir kt.), o vėliau ji gali būti naudojama prieigai prie internetinių administracinių paslaugų.

21. Be to, naudojant veido atpažinimo technologiją tapatybei patvirtinti gali būti siekiama kontroliuoti fizinę prieigą prie vienos ar daugiau iš anksto nustatytų vietų, pavyzdžiui, įėjimų į pastatus arba konkrečių perėjimo punktų. Ši funkcija, pavyzdžiui, įgyvendinama tam tikruose sienos kirtimo tikslu atliekamuose duomenų tvarkymo procesuose, kai asmens veidas patikros vietos įrenginyje lyginamas su asmens tapatybės dokumente (pase arba saugiame leidime gyventi) išsaugotu veidu.

Veido atpažinimo technologijos naudojimo tapatybei nustatyti pavyzdžiai

22. Tapatybės nustatymas gali būti taikomas daugeliu, dar įvairesnių būdų (tai visų pirma apima toliau išvardytus naudojimo būdus, kurie šiuo metu naudojami, su kuriais eksperimentuojama ar kuriuos planuojama įgyvendinti ES, tačiau jais neapsiriboja):

- neatpažinto asmens (nukentėjusiojo, įtariamojo ir kt.) tapatybės paieška nuotraukų duomenų bazėje;
- asmens judėjimo viešojoje erdvėje stebėsena. Jo veidas lyginamas su stebimoje zonoje esančių ar buvusių asmenų biometrinių duomenų šablonais, pavyzdžiui, kai paliekamas be priežiūros bagažas arba po to, kai įvykdomas nusikaltimas;
- asmens maršruto ir paskesnių kontaktų su kitais asmenimis atgaminimas, atliekant atidėtąjį tų pačių elementų palyginimą, kad būtų galima nustatyti, pavyzdžiui, asmens kontaktus;
- nuotolinis biometrinis ieškomų asmenų tapatybės nustatymas viešosiose erdvėse. Atliekama visų vaizdo apsaugos kameromis tiesiogiai užfiksuotų veidų kryžminė patikra su saugumo tarnybų turima duomenų baze realiuoju laiku;
- automatinis žmonių atpažinimas atvaizde, siekiant nustatyti, pavyzdžiui, jų santykius socialiniame tinkle, kuriame jis naudojamas. Atvaizdas lyginamas su visų tinklo dalyvių, sutikusių naudotis šia funkcija, šablonais, kad būtų galima pateikti pasiūlymų dėl nominalaus šių ryšių nustatymo;
- galimybė naudotis paslaugomis, kai tam tikri bankomatai atpažįsta savo klientus, palygindami kameroje užfiksuotą veidą su banko veido atvaizdų duomenų baze;
- keleivio maršruto sekimas tam tikrame kelionės etape. Realiuoju laiku apskaičiuotas bet kurio asmens, užsiregistravusio prie tam tikruose kelionės etapuose esančių vartų (bagažo pridavimo punktuose, prie įlaipinimo vartų ir kt.), šablonas lyginamas su anksčiau sistemoje užregistruotais asmenų šablonais.

23. Be veido atpažinimo technologijos naudojimo teisėsaugos srityje, atsižvelgiant į pastebėtą didelę taikymo būdų įvairovę, tikrai reikia surengti išsamias diskusijas ir parengti politinį požiūrį, kad būtų užtikrintas nuoseklumas ir atitiktis ES *acquis* duomenų apsaugos srityje.

2.3 Patikimumas, tikslumas ir rizika duomenų subjektams

24. Kaip ir kiekviena technologija, veido atpažinimo technologija taip pat gali kelti sunkumų ją įgyvendinant, visų pirma kiek tai susiję su jos patikimumu ir veiksmingumu tapatybės patvirtinimo ar

nustatymo požiūriu, taip pat su bendru pirminių duomenų kokybės ir tikslumo bei veido atpažinimo technologijos apdorojimo rezultatų klausimu.

25. Tokie technologiniai iššūkiai susijusiems duomenų subjektams kelia ypatingą riziką, kuri teisėsaugos srityje yra dar didesnė arba rimtesnė, atsižvelgiant į galimą teisinį arba kitokį panašų reikšmingą poveikį duomenų subjektams. Šiomis aplinkybėmis taip pat naudinga pabrėžti, kad veido atpažinimo technologijos *ex post* naudojimas savaime nėra saugesnis, nes asmenys gali būti stebimi skirtingais laikotarpiais ir skirtingose vietose. Todėl *ex post* naudojimas taip pat kelia konkrečią riziką, kurią reikia vertinti kiekvienu konkrečiu atveju[7].

26. Kaip 2019 m. ataskaitoje nurodė ES pagrindinių teisių agentūra, „nustatyti būtiną veido atpažinimo programinės įrangos tikslumo lygį yra sudėtinga: yra daug įvairių būdų įvertinti tikslumą, taip pat priklausomai nuo jos naudojimo paskirties, tikslo ir aplinkybių. Taikant šią technologiją vietose, kuriose lankosi milijonai žmonių, pavyzdžiui, traukinių stotyse ar oro uostuose, santykinai nedidelė klaidų dalis (pvz., 0,01 %)[8] vis tiek reiškia, kad šimtai žmonių yra žymimi klaidingai. Be to, kaip aprašyta 3 skirsnyje, tam tikrų kategorijų asmenys gali būti klaidingai pažymėti kaip atitiktis dažniau nei kitų kategorijų asmenys. Klaidų lygius galima apskaičiuoti ir išaiškinti įvairiai, todėl reikia elgtis atsargiai. Be to, kalbant apie tikslumą ir klaidas, ypač teisėsaugos tikslams svarbūs klausimai yra susiję su tuo, kaip lengvai galima apgauti sistemą, pavyzdžiui, naudojant suklastotus veidų atvaizdus (tai vadinama apsimetinėjimu).“[9]

27. Atsižvelgiant į tai, EDAV nuomone, svarbu priminti, kad veido atpažinimo technologija, neatsižvelgiant į tai, ar ji naudojama tapatybės patvirtinimo ar tapatybės nustatymo tikslais, nenumato galutinio rezultato, o grindžiama tikimybėmis, kad du veidai arba veidų atvaizdai atitinka tą patį asmenį[10]. Šis rezultatas yra dar prastesnis, kai veido atpažinimui naudojami nekokybiški biometrinių duomenų pavyzdžiai. Prastą kokybę gali lemti įvesties vaizdų neryškumas, maža kameros skiriamoji geba, judėjimas ir silpnas apšvietimas. Kiti aspektai, darantys didelę įtaką rezultatams, yra paplitimas ir apsimetinėjimas, pavyzdžiui, kai nusikaltėliai stengiasi nepatekti į kamerų lauką arba apgauti veido atpažinimo technologiją. Iš įvairių tyrimų taip pat matyti, kad tokie statistiniai algoritminio duomenų tvarkymo rezultatai taip pat gali būti šališki, ypač dėl pirminių duomenų kokybės, mokymo duomenų bazių ar kitų veiksnių, kaip antai naudojimo vietos pasirinkimo. Be to, reikėtų pabrėžti veido atpažinimo technologijos poveikį kitoms pagrindinėms teisėms, pavyzdžiui, teisei į privatų ir šeimos gyvenimą, saviraiškos ir informacijos laisvei, susirinkimų ir asociacijų laisvei ir kt.

28. Todėl labai svarbu, kad į veido atpažinimo technologijos patikimumą ir tikslumą būtų atsižvelgiama kaip į kriterijus vertinant atitiktį pagrindiniams duomenų apsaugos principams, kaip nustatyta Teisėsaugos direktyvos 4 straipsnyje, ypač kai tai susiję su sąžiningumu ir tikslumu.

29. Pabrėždama, kad kokybiški duomenys yra būtini kokybiškiems algoritmams, EDAV taip pat pabrėžia, kad duomenų valdytojai, vykdydami savo atskaitomybės pareigą, turi reguliariai ir sistemingai vertinti algoritminį duomenų tvarkymą, kad visų pirma užtikrintų tokio asmens duomenų tvarkymo rezultatų tikslumą, sąžiningumą ir patikimumą. Asmens duomenys, naudojami veido atpažinimo technologijos sistemų vertinimo, mokymo ir tolesnio tobulinimo tikslais, gali būti tvarkomi tik remiantis tinkamu teisiniu pagrindu ir laikantis bendrųjų duomenų apsaugos principų.

[7] Žr. III priede pateiktus pavyzdžius.

[8] Šis tikslumo lygis grindžiamas cituojama ataskaita ir yra daug geresnis nei dabartinis algoritmų veiksmingumas taikant veido atpažinimo technologiją.

[9] Veido atpažinimo technologija: pagrindinių teisių aspektai teisėsaugos kontekste, ES pagrindinių teisių agentūra, 2019 m. lapkričio 21 d.

[10] Ši tikimybė vadinama patikimumo įvertinimu.

3 TAIKYTINA TEISINĖ SISTEMA

30. Veido atpažinimo technologijų naudojimas yra iš esmės susijęs su asmens duomenų tvarkymu, įskaitant specialių kategorijų duomenis. Be to, ši technologija daro tiesioginį ar netiesioginį poveikį tam tikroms pagrindinėms teisėms, įtvirtintoms ES pagrindinių teisių chartijoje. Tai ypač svarbu teisėsaugos ir baudžiamosios teisenos srityje. Todėl bet koks veido atpažinimo technologijų naudojimas turėtų būti vykdomas griežtai laikantis taikytinos teisinės sistemos.

31. Toliau pateiktą informaciją ketinama naudoti vertinant būsimas teisėkūros ir administracines priemones, taip pat įgyvendinant esamus teisės aktus kiekvienu konkrečiu atveju, kai tai susiję su veido atpažinimo technologijos naudojimu. Atitinkamų reikalavimų svarba priklauso nuo konkrečių aplinkybių. Kadangi ne visos būsimos aplinkybės gali būti numatytos, laikoma, kad ši informacija tik pagalbinė ir sąrašo nereikėtų laikyti baigtiniu.

3.1 Bendroji teisinė sistema. ES pagrindinių teisių chartija ir Europos žmogaus teisių konvencija (EŽTK)

3.1.1 Chartijos taikymas

32. ES pagrindinių teisių chartija (toliau – Chartija) skirta Sąjungos institucijoms, įstaigoms, organams ir agentūroms bei valstybėms narėms, kai jos įgyvendina Sąjungos teisę.

33. Reglamentuojant biometrinių duomenų tvarkymą teisėsaugos tikslais pagal Teisėsaugos direktyvos 1 straipsnio 1 dalį neišvengiamai kyla klausimas dėl pagrindinių teisių laikymosi, visų pirma teisės į privatų gyvenimą ir komunikacijos slaptumą pagal Chartijos 7 straipsnį ir teisės į asmens duomenų apsaugą pagal Chartijos 8 straipsnį.

34. Filmuotos vaizdo medžiagos, kurioje matomi fiziniai asmenys ir jų veidai, rinkimas ir analizė reiškia, kad vyksta asmens duomenų tvarkymas. Techniškai apdorojant vaizdą, apdorojami ir biometriniai duomenys. Techninis su fizinio asmens veidu susijusių duomenų tvarkymas laiko ir vietos atžvilgiu leidžia daryti išvadas dėl atitinkamų asmenų privataus gyvenimo. Šiose išvadose gali būti nuorodų į rasinę ar etninę kilmę, sveikatos būklę, religiją, kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ar kitokį judėjimą, vykdomą veiklą, tų asmenų socialinius ryšius ir socialinę aplinką, kurioje jie lankosi. Didžioji dalis informacijos, kuri gali būti atskleista taikant veido atpažinimo technologiją, aiškiai rodo galimą poveikį Chartijos 8 straipsnyje nustatytai teisei į asmens duomenų apsaugą, taip pat Chartijos 7 straipsnyje nustatytai teisei į privatų gyvenimą.

35. Tokiomis aplinkybėmis taip pat negalima atmesti galimybės, kad nagrinėjamų biometrinių (veido) duomenų rinkimas, analizė ir tolesnis tvarkymas gali turėti įtakos žmonių veikimo laisvei, net jei tas veiksmas visiškai atitiktų laisvos ir atviros visuomenės principus. Tai taip pat gali turėti rimtų pasekmių jų naudojimuisi pagrindinėmis teisėmis, pavyzdžiui, teise į minties, sąžinės ir religijos laisvę, taikių susirinkimų ir asociacijų laisve, pagal Chartijos 1, 10, 11 ir 12 straipsnius. Toks duomenų tvarkymas taip pat susijęs su kitais pavojais, pavyzdžiui, rizika, kad bus piktnaudžiaujama atitinkamų institucijų surinkta asmenine informacija dėl neteisėtos prieigos prie asmens duomenų ir jų naudojimo, saugumo pažeidimo ir kt. Rizika neretai priklauso nuo duomenų tvarkymo ir jo aplinkybių, pavyzdžiui, rizikos, kad policijos pareigūnai ar kiti leidimo neturintys asmenys gali neteisėtai susipažinti su asmens duomenimis ir jais naudotis. Tačiau kai kurių rūšių rizika tiesiog būdinga unikaliam biometrinių duomenų pobūdžiui. Skirtingai nei adreso ar telefono numerio, duomenų subjektas negali pakeisti savo unikalių savybių, pvz., veido ar akies rainelės. Neteisėtos prieigos prie biometrinių duomenų arba atsitiktinio jų

paskelbimo atveju kiltų pavojus, kad duomenų kaip slaptažodžių arba kriptografinių raktų naudojimas taptų nebesaugus arba jie galėtų būti panaudoti kitai neteisėtai stebėjimo veiklai, kenkiančiai duomenų subjektui.

3.1.2 Chartijoje nustatytų teisių suvaržymas

36. Biometrinių duomenų tvarkymas bet kokiomis aplinkybėmis pats savaime yra didelis suvaržymas. Tai nepriklauso nuo rezultato, pvz., teigiamos atitikties. Duomenų tvarkymas – tai suvaržymas, net jeigu biometrinių duomenų šablonas iš karto ištrinamas po to, kai palyginus duomenis su policijos duomenų baze nustatoma, kad atitikčių nėra.

37. Duomenų subjektų pagrindinių teisių suvaržymas gali būti pagrįstas teisės aktu, kuriuo siekiama apriboti atitinkamą pagrindinę teisę arba kuriuo ji apribojama[11]. Suvaržymą taip pat gali lemti valdžios institucijos veiksmas, turintis tokį patį tikslą ar poveikį, arba net privataus subjekto, kuriam pagal įstatymą pavesta vykdyti viešosios valdžios funkciją ir viešuosius įgaliojimus, veiksmas.

38. Teisėkūros priemone, kuri yra asmens duomenų tvarkymo teisinis pagrindas, tiesiogiai varžomos Chartijos 7 ir 8 straipsniais garantuojamos teisės[12].

39. Biometrinių duomenų ir ypač veido atpažinimo technologijos naudojimas daugeliu atvejų taip pat daro poveikį Chartijos 1 straipsniu garantuojamai teisei į žmogaus orumą. Žmogaus orumui užtikrinti būtina, kad su žmonėmis nebūtų elgiamasi kaip su daiktais. Taikant veido atpažinimo technologiją, apskaičiuojamos egzistencinės ir labai asmeniškos veido savybės, veido bruožai, juos pateikiant kompiuterio skaitoma forma, kad būtų galima juos naudoti kaip žmogaus numerį arba asmens tapatybės kortelę, taip įdaiktinant veidą.

40. Tokiu duomenų tvarkymu taip pat gali būti varžomos ir kitos pagrindinės teisės, pavyzdžiui, teisės pagal Chartijos 10, 11 ir 12 straipsnius, jei atgrasomasis poveikis numatomas arba pasireiškia dėl atitinkamo teisėsaugos institucijų vykdomo stebėjimo vaizdo kameromis.

41. Be to, taip pat reikėtų atidžiai apsvarstyti galimą riziką, teisėsaugos institucijoms naudojant veido atpažinimo technologijas kylančią teisei į teisingą bylos nagrinėjimą ir nekaltumo prezumpcijai pagal Chartijos 47 ir 48 straipsnius. Veido atpažinimo technologijos taikymo rezultatas, pvz., atitiktis, gali lemti ne tik tolesnį asmens stebėjimą, kurį vykdo policija, bet ir būti lemiamu įrodymu teismo procese. Todėl veido atpažinimo technologijos trūkumai, pavyzdžiui, galimas šališkumas, diskriminacija ar neteisingas tapatybės nustatymas (toliau – klaidingas teigiamas rezultatas), gali turėti rimtų pasekmių ir baudžiamajam procesui. Be to, vertinant įrodymus pirmenybė gali būti teikiama veido atpažinimo technologijos taikymo rezultatui, net jei yra prieštaringų įrodymų (toliau – automatizavimo šališkumas).

3.1.3 Suvaržymo pateisinimas

42. Pagal Chartijos 52 straipsnio 1 dalį bet koks pagrindinių teisių ir laisvių įgyvendinimo apribojimas turi būti numatytas įstatymo ir nekeisti šių teisių ir laisvių esmės. Remiantis proporcingumo principu, apribojimai galimi tik tuo atveju, kai jie būtini ir tikrai atitinka Europos Sąjungos pripažintus bendrus interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

3.1.3.1 Numatyta įstatymo

43. Chartijos 52 straipsnio 1 dalyje nustatytas konkretaus teisinio pagrindo reikalavimas. Šis teisinis pagrindas turi būti pakankamai aiškus, kad piliečiams būtų tinkamai nurodytos sąlygos ir aplinkybės,

[11] 1992 m. spalio 28 d. ESTT sprendimas *Ter Voort*, C-219/91, Rink. p. I-05485, 36f punktas; 1998 m. balandžio 28 d. ESTT sprendimas *Metronome*, C-200/96, Rink. p. 1998 I-1953, 28 punktas.

[12] ESTT sprendimas byloje C-594/12, 36 punktas; ESTT sprendimas byloje C-291/12, 23 ir paskesni punktai.

kuriomis valdžios institucijos yra įgaliotos imtis bet kokių duomenų rinkimo ir slapto sekimo priemonių[13]. Jame turi būti pakankamai aiškiai nurodyta valdžios institucijoms suteiktos atitinkamos veiksmų laisvės apimtis ir įgyvendinimo būdas, kad asmenims būtų užtikrinta minimali apsauga, į kurią jie turi teisę pagal teisinės valstybės principą demokratinėje visuomenėje[14]. Be to, teisėtumui reikia tinkamų apsaugos priemonių, kuriomis būtų užtikrinama, kad visų pirma būtų gerbiama asmens teisė pagal Chartijos 8 straipsnį. Šie principai taip pat taikomi asmens duomenų tvarkymui veido atpažinimo technologijos sistemų vertinimo, mokymo ir tolesnio tobulinimo tikslais.

44. Atsižvelgiant į tai, kad biometriniai duomenys, kai jie tvarkomi siekiant nustatyti konkretaus fizinio asmens tapatybę, laikomi specialių kategorijų duomenimis, išvardytais Teisėsaugos direktyvos 10 straipsnyje, dėl skirtingų veido atpažinimo technologijos taikymo būdų daugeliu atvejų reikėtų priimti specialų teisės aktą, kuriame būtų tiksliai aprašytas taikymo būdas ir jo naudojimo sąlygos. Tai visų pirma apima įvairių rūšių nusikalstamumą ir, kai taikytina, atitinkamą tų nusikaltimų sunkumo ribą, kad, be kita ko, būtų veiksmingai užkirstas kelias smulkiems nusikaltimams[15].

3.1.3.2 Chartijos 7 ir 8 straipsniuose įtvirtintos pagrindinės teisės į privatų gyvenimą ir asmens duomenų apsaugą esmė

45. Taikant pagrindinių teisių apribojimus, būdingus kiekvienai situacijai, vis tiek turi būti užtikrinta, kad būtų gerbiama konkrečios teisės esmė. Esmė yra tai, kuo grindžiama atitinkama pagrindinė teisė[16]. Žmogaus orumas taip pat turi būti gerbiamas, net jei teisė ribojama[17].

46. Galimi požymiai, kad pažeista neliečiama esmė:

- nuostata, kuria nustatomi apribojimai, neatsižvelgiant į asmens asmeninį elgesį ar išimtines aplinkybes[18];
- kreipimasis į teismus nėra įmanomas arba jam trukdoma[19];
- prieš pradedant taikyti griežtą apribojimą neatsižvelgiama į atitinkamo asmens aplinkybes[20];
- atsižvelgiant į Chartijos 7 ir 8 straipsniuose numatytas teises, be plataus komunikacijos metaduomenų rinkinio, žinių apie elektroninės komunikacijos turinį įgijimas galėtų pažeisti šių teisių esmę[21];
- atsižvelgiant į Chartijos 7, 8 ir 11 straipsniuose numatytas teises, teisės aktai, pagal kuriuos reikalaujama, kad prieigos prie internetinių viešųjų ryšių paslaugų teikėjai ir prieglobos paslaugų teikėjai bendrai ir nediferencijuotai išsaugotų, be kita ko, su šiomis paslaugomis susijusius asmens duomenis[22];
- kalbant apie Chartijos 8 straipsnyje numatytas teises, pagrindinių duomenų apsaugos ir duomenų saugumo principų nebuvimas taip pat galėtų pažeisti teisės esmę[23].

---

[13] EŽTT, *Shimovolos prieš Rusiją*, 68 punktas; *Vukota-Bojić prieš Šveicariją*.
[14] EŽTT, *Piechowicz prieš Lenkiją*, 212 punktas.
[15] Žr., pavyzdžiui, ESTT sprendimus *Ligue des droits humains* (C-817/19, 151f punktas), *Ministerio Fiscal* (C-207/16, 56 punktas).
[16] 2010 m. gruodžio 22 d. ESTT sprendimas byloje C-279/09, Rink. p. I-13849, 60 punktas.
[17] Su Pagrindinių teisių chartija susiję išaiškinimai, I antraštinė dalis, 1 straipsnio išaiškinimas (OL C 303, 2007 12 14, p. 17–35).
[18] ESTT sprendimas byloje C-601/15, 52 punktas.
[19] 2010 m. spalio 5 d. ESTT sprendimas byloje C-400/10, Rink. p. I-08965, 55 punktas.
[20] 2006 m. kovo 23 d. ESTT sprendimas byloje C-408/03, Rink. p. I-02647, 68 punktas.
[21] ESTT sprendimas *Tele2 Sverige*, 203/15, 101 punktas, su nuoroda į ESTT sprendimą bylose C-293/12 ir C-594/12, 39 punktas.
[22] ESTT sprendimas *La Quadrature du Net*, C-512/18, 209 ir paskesni punktai.
[23] ESTT sprendimas byloje C-594/12, 40 punktas.

3.1.3.3 Teisėtas tikslas

47. Kaip jau paaiškinta 3.1.3 punkte, pagrindinių teisių apribojimai turi iš tikrųjų atitikti Europos Sąjungos pripažinto bendrojo intereso tikslus arba patenkinti poreikį apsaugoti kitų asmenų teises ir laisves.

48. Sąjunga pripažįsta tiek Europos Sąjungos sutarties 3 straipsnyje nurodytus tikslus, tiek kitus konkrečiomis Sutarčių nuostatomis saugomus interesus[24], t. y., *inter alia*, laisvės, saugumo ir teisingumo erdvę, nusikalstamumo prevenciją ir kovą su juo. Santykiuose su likusiu pasauliu Sąjunga turėtų prisidėti prie taikos ir saugumo bei žmogaus teisių apsaugos.

49. Būtinybė apsaugoti kitų asmenų teises ir laisves susijusi su asmenų teisėmis, kurios saugomos pagal Europos Sąjungos arba jos valstybių narių teisę. Vertinimas turi būti atliekamas siekiant suderinti atitinkamų teisių apsaugos reikalavimus ir užtikrinti teisingą jų pusiausvyrą[25].

3.1.3.4 Būtinumo ir proporcingumo kriterijus

50. Kai kalbama apie pagrindinių teisių suvaržymą, gali paaiškėti, kad nacionalinės ir Sąjungos teisės aktų leidėjo diskrecija yra ribota. Tai priklauso nuo daugelio veiksnių, įskaitant atitinkamą sritį, Chartijos garantuojamos atitinkamos teisės pobūdį, suvaržymo pobūdį bei rimtumą ir suvaržymu siekiamą tikslą[26]. Teisėkūros priemonės turi būti tinkamos siekiant teisėtų tikslų, kurių siekiama atitinkamais teisės aktais. Be to, priemonė neturi viršyti to, kas yra tinkama ir būtina šiems tikslams pasiekti[27]. Bendrojo intereso tikslas, kad ir koks svarbus jis būtų, pats savaime nepateisina pagrindinės teisės apribojimo[28].

51. Pagal suformuotą ESTT jurisprudenciją nukrypti leidžiančios nuostatos ir apribojimai, susiję su asmens duomenų apsauga, turi būti taikomi tik tiek, kiek tai tikrai būtina[29]. Tai taip pat reiškia, kad nėra mažesnio poveikio suvaržymo priemonių, kuriomis būtų galima pasiekti tikslą. Priklausomai nuo konkretaus tikslo, reikia atidžiai nustatyti ir įvertinti galimas alternatyvas, tokias kaip papildomi darbuotojai, dažnesnis policijos patruliavimas ar papildomas gatvių apšvietimas. Teisėkūros priemonėmis asmenys, kuriems jos skirtos, turėtų būti diferencijuojami ir aprėpiami atsižvelgiant į tikslą, pavyzdžiui, kovą su sunkiais nusikaltimais. Jeigu priemonė taikoma visiems asmenims bendrai be tokio diferencijavimo, apribojimo ar išimties, suvaržymas suintensyvėja[30]. Jis taip pat suintensyvėja, jei duomenų tvarkymas apima didelę gyventojų dalį[31].

52. Asmens duomenų apsauga vykdant Chartijos 8 straipsnio 1 dalyje nustatytą aiškią pareigą yra ypač svarbi Chartijos 7 straipsnyje įtvirtintai teisei į privataus gyvenimo gerbimą[32]. Teisės aktuose turi būti nustatytos aiškios ir tikslios taisyklės, kuriomis reglamentuojama atitinkamos priemonės taikymo sritis ir taikymas ir apsaugos priemonės, kad asmenys, kurių duomenys buvo tvarkomi, turėtų pakankamas

---

[24] Su Pagrindinių teisių chartija susiję išaiškinimai, I antraštinė dalis, 52 straipsnio išaiškinimas (OL C 303, 2007 12 14, p. 17–35).

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

[26] ESTT sprendimas byloje C-594/12, 47 punktas, kartu atsižvelgiant į šiuos šaltinius: pagal analogiją dėl EŽTK 8 straipsnio žr. Europos žmogaus teisių teismo sprendimo *S. ir Marper prieš Jungtinę Karalystę* [GC], Nr. 30562/04 ir 30566/04, 102 punktą, ECHR 2008-V.

[27] ESTT sprendimas byloje C-594/12, 46 punktas, kartu atsižvelgiant į šiuos šaltinius: Sprendimo *Afton Chemical*, C-343/09, EU:C:2010:419, 45 punktą; Sprendimo *Volker und Markus Schecke ir Eifert*, EU:C:2010:662, 74 punktą; Sprendimo *Nelson ir kt.*, C-581/10 ir C-629/10, EU:C:2012:657, 71 punktą; Sprendimo *Sky Österreich*, C-283/11, EU:C:2013:28, 50 punktą; Sprendimo *Schaible*, C-101/12, EU:C:2013:661, 29 punktą.

[28] ESTT sprendimas byloje C-594/12, 51 punktas.

[29] ESTT sprendimas byloje C-594/12, 52 punktas, kartu atsižvelgiant į šiuos šaltinius: Sprendimo *IPI*, C-473/12, EU:C:2013:715, 39 punktą ir jame nurodytą jurisprudenciją.

[30] ESTT sprendimas byloje C-594/12, 57 punktas.

[31] ESTT sprendimas byloje C-594/12, 56 punktas.

[32] ESTT sprendimas byloje C-594/12, 53 punktas.

garantijas veiksmingai apsaugoti savo asmens duomenis nuo piktnaudžiavimo pavojaus ir nuo bet kokios neteisėtos prieigos prie tų duomenų ar jų naudojimo[33]. Tokių apsaugos priemonių poreikis yra dar didesnis tais atvejais, kai asmens duomenys tvarkomi automatiškai ir kai kyla didelė neteisėtos prieigos prie duomenų rizika[34]. Be to, vidaus ar išorės, pvz., teismo, leidimas naudoti veido atpažinimo technologiją taip pat gali būti viena iš apsaugos priemonių ir tam tikrais didelio suvaržymo atvejais gali pasirodyti būtinas[35].

53. Nustatytos taisyklės turi būti pritaikytos prie konkrečios situacijos, pavyzdžiui, tvarkomų duomenų kiekio, duomenų pobūdžio[36] ir neteisėtos prieigos prie duomenų pavojaus. Todėl reikia taisyklių, kuriomis visų pirma būtų aiškiai ir griežtai reglamentuojama atitinkamų duomenų apsauga ir saugumas, siekiant užtikrinti visišką jų vientisumą ir konfidencialumą[37].

54. Kalbant apie duomenų valdytojo ir duomenų tvarkytojo santykius, duomenų tvarkytojams neturėtų būti leidžiama, nustatant asmens duomenims taikomą saugumo lygį, atsižvelgti tik į ekonominius sumetimus; tai galėtų kelti pavojų pakankamai aukštam apsaugos lygiui[38].

55. Teisės akte turi būti nustatytos materialinės ir procedūrinės sąlygos bei objektyvūs kriterijai, pagal kuriuos nustatomos kompetentingų institucijų prieigos prie duomenų ir jų tolesnio naudojimo ribos. Prevencijos, aptikimo ar baudžiamojo persekiojimo tikslais atitinkamos nusikalstamos veikos turėtų būti laikomos pakankamai sunkiomis, kad būtų galima pateisinti šio naudojimosi pagrindinėmis teisėmis, įtvirtintomis, pavyzdžiui, Chartijos 7 ir 8 straipsniuose, suvaržymo mastą ir rimtumą[39].

56. Duomenys turi būti tvarkomi taip, kad būtų užtikrintas ES duomenų apsaugos taisyklių taikomumas ir poveikis, visų pirma tų, kurios numatytos Chartijos 8 straipsnyje, kuriame teigiama, kad apsaugos ir saugumo reikalavimų laikymąsi kontroliuoja nepriklausoma institucija. Tokioje situacijoje gali būti svarbi geografinė vieta, kurioje vykdomas duomenų tvarkymas[40].

57. Kalbant apie skirtingus asmens duomenų tvarkymo etapus, reikėtų atskirti duomenų kategorijas pagal jų galimą naudingumą siekiant norimo tikslo arba atsižvelgiant į susijusius asmenis[41]. Duomenų tvarkymo sąlygų nustatymas, pavyzdžiui, saugojimo laikotarpio nustatymas, turi būti grindžiamas objektyviais kriterijais, siekiant užtikrinti, kad suvaržymas neviršytų to, kas tikrai būtina[42].

58. Atsižvelgiant į kiekvieną situaciją, atliekant būtinumo ir proporcingumo vertinime reikia nustatyti ir apsvarstyti visus padarinius, susijusius su kitų pagrindinių teisių taikymo sritimi, pavyzdžiui, žmogaus orumu pagal Chartijos 1 straipsnį, minties, sąžinės ir religijos laisve pagal Chartijos 10 straipsnį,

---

[33] ESTT sprendimas byloje C-594/12, 54 punktas, kartu atsižvelgiant į šiuos šaltinius: pagal analogiją dėl EŽTK 8 straipsnio žr. 2008 m. liepos 1 d. Europos Žmogaus teisių teismo sprendimo *Liberty ir kt. prieš Jungtinę Karalystę*, Nr. 58243/00, 62 ir 63 punktus; Sprendimo *Rotaru prieš Rumuniją* 57–59 punktus ir Sprendimo *S. ir Marper prieš Jungtinę Karalystę* 99 punktą.

[34] ESTT sprendimas byloje C-594/12, 55 punktas, kartu atsižvelgiant į šiuos šaltinius: pagal analogiją dėl EŽTK 8 straipsnio žr. Sprendimo *S. ir Marper prieš Jungtinę Karalystę*, 103 punktą, ir 2013 m. balandžio 18 d. Sprendimo *M. K. prieš Prancūziją*, Nr. 19522/09, 35 punktą.

[35] EŽTT, *Szabó ir Vissy prieš Vengriją*, 73–77 punktai.

[36] Taip pat žr. griežtesnius reikalavimus techninėms ir organizacinėms priemonėms tvarkant specialių kategorijų duomenis (Teisėsaugos direktyvos 29 straipsnio 1 dalis).

[37] ESTT sprendimas byloje C-594/12, 66 punktas.

[38] ESTT sprendimas byloje C-594/12, 67 punktas.

[39] ESTT sprendimas C-594/12, 60 ir 61 punktai.

[40] ESTT sprendimas byloje C-594/12, 68 punktas.

[41] ESTT sprendimas byloje C-594/12, 63 punktas.

[42] ESTT sprendimas byloje C-594/12, 64 punktas.

saviraiškos laisve pagal Chartijos 11 straipsnį ir susirinkimų ir asociacijų laisve pagal Chartijos 12 straipsnį.

59. Be to, vertinant sunkumą turi būti laikoma, kad jei duomenys sistemingai tvarkomi be duomenų subjektų žinios, tikėtina, kad įsitvirtins bendras nuolatinis stebėjimas[43]. Dėl to kai kurių arba visų atitinkamų pagrindinių teisių atžvilgiu gali atsirasti atgrasomasis poveikis.

60. Siekiant palengvinti ir praktiškai įgyvendinti su veido atpažinimu susijusių teisėkūros priemonių būtinumo ir proporcingumo vertinimą teisėsaugos srityje, nacionalinės ir Sąjungos teisės aktų leidėjai galėtų pasinaudoti turimomis praktinėmis priemonėmis, specialiai sukurtomis šiai užduočiai atlikti. Visų pirma būtų galima naudoti Europos duomenų apsaugos priežiūros pareigūno pateiktą būtinumo ir proporcingumo priemonių rinkinį[44].

3.1.3.5 Chartijos 52 straipsnio 3 dalis, 53 straipsnis (apsaugos lygis, taip pat palyginti su EŽTK lygiu)

61. Pagal Chartijos 52 straipsnio 3 dalį ir 53 straipsnį Chartijos teisių, atitinkančių EŽTK garantuojamas teises, prasmė ir taikymo sritis turi būti tokia pati, kaip nustatyta EŽTK. Nors visų pirma Chartijos 7 straipsniui lygiavertį atitikmenį galima rasti EŽTK, apie Chartijos 8 straipsnį to pasakyti negalima[45]. Chartijos 52 straipsnio 3 dalimi nedraudžiama Sąjungos teisės aktais nustatyti platesnę apsaugą. Kadangi EŽTK nėra oficialiai į ES teisę įtrauktas teisinis dokumentas, ES teisės aktai turi būti priimami atsižvelgiant į Chartijoje įtvirtintas pagrindines teises[46].

62. Pagal EŽTK 8 straipsnį valdžios institucija negali varžyti naudojimosi šia teise į pagarbą privačiam ir šeimos gyvenimui, išskyrus atvejus, kai tai daroma pagal įstatymą ir kai tai būtina demokratinėje visuomenėje nacionalinio saugumo, visuomenės saugumo ar šalies ekonominės gerovės interesais, siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, apsaugoti sveikatą ar moralę arba kitų asmenų teises ir laisves.

63. EŽTK taip pat nustatyti standartai, susiję su tuo, kaip galima taikyti apribojimus. Be teisinės valstybės principo, vienas iš pagrindinių reikalavimų yra nuspėjamumas. Siekiant įvykdyti nuspėjamumo reikalavimą, teisės aktai turėtų būti pakankamai aiškūs, kad suteiktų piliečiams pakankamai informacijos, kokiais atvejais ir kokiomis sąlygomis valdžios institucijos turi teisę taikyti tokias priemones[47]. Šį reikalavimą pripažįsta ESTT ir ES duomenų apsaugos teisės aktai (žr. 3.2.1.1 skirsnį).

64. Papildomai patikslinant EŽTK 8 straipsnyje nustatytas teises, taip pat turi būti visapusiškai laikomasi Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[48] nuostatų. Vis dėlto reikia atsižvelgti į tai, kad, atsižvelgiant į galiojančią Sąjungos teisę, šios nuostatos yra tik minimalusis standartas.

3.2 Specialioji teisinė sistema. Teisėsaugos direktyva

[43] ESTT sprendimas byloje C-594/12, 37 punktas.
[44] Europos duomenų apsaugos priežiūros pareigūnas, „Priemonių, kuriomis ribojama pagrindinė teisė į asmens duomenų apsaugą, būtinumo vertinimas. Priemonių rinkinys“ (2017 04 11); Europos duomenų apsaugos priežiūros pareigūnas, „EDAPP gairės dėl priemonių, kuriomis ribojamos pagrindinės teisės į privatų gyvenimą ir asmens duomenų apsaugą, proporcingumo vertinimo“ (2019 12 19).
[45] ESTT sprendimas *Tele2 Sverige*, C-203/15, 129 punktas.
[46] ESTT sprendimas byloje C-311/18, 99 punktas.
[47] 2007 m. balandžio 3 d. Europos Žmogaus Teisių Teismo sprendimas *COPLAND prieš JUNGTINĘ KARALYSTĘ*, Ieškinio Nr. 62617/00, 46 punktas.
[48] Europos Tarybos 108-oji konvencija.

65. Teisėsaugos direktyvoje numatyta tam tikra veido atpažinimo technologijos naudojimo sistema. Visų pirma, Teisėsaugos direktyvos 3 straipsnio 13 punkte apibrėžiama sąvoka „biometriniai duomenys“[49]. Išsamesnė informacija pateikiama 2.1 skirsnyje. Antra, 8 straipsnio 2 dalyje paaiškinama, kad tam, kad bet koks duomenų tvarkymas būtų teisėtas, jis turi būti ne tik būtinas Teisėsaugos direktyvos 1 straipsnio 1 dalyje nurodytais tikslais, bet ir reglamentuotas nacionalinėje teisėje, kurioje nurodomi bent jau duomenų tvarkymo tikslai, tvarkytini asmens duomenys ir duomenų tvarkymo paskirtis. Kitos nuostatos, ypač svarbios biometriniams duomenims, yra Teisėsaugos direktyvos 10 ir 11 straipsniai. Direktyvos 10 straipsnis turi būti aiškinamas kartu su jos 8 straipsniu[50]. Visada turėtų būti laikomasi asmens duomenų tvarkymo principų, nustatytų Teisėsaugos direktyvos 4 straipsnyje, ir jais turėtų būti vadovaujamasi atliekant bet kokį galimo biometrinio duomenų tvarkymo naudojant veido atpažinimo technologiją vertinimą.

3.2.1 Specialių kategorijų duomenų tvarkymas teisėsaugos tikslais

66. Pagal Teisėsaugos direktyvos 10 straipsnį specialių kategorijų duomenų, pavyzdžiui, biometrinių duomenų, tvarkymas leidžiamas tik tais atvejais, kai tai tikrai būtina ir jei taikomos atitinkamos duomenų subjekto teisių ir laisvių apsaugos priemonės. Be to, tai leidžiama tik tais atvejais, kai tai leidžiama pagal Sąjungos arba valstybės narės teisę, siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus arba kai toks tvarkymas yra susijęs su duomenimis, kuriuos duomenų subjektas yra aiškiai paskelbęs viešai. Šioje bendrojoje nuostatoje pabrėžiamas specialių kategorijų duomenų tvarkymo jautrumas.

3.2.1.1 Įgaliota pagal Sąjungos arba valstybės narės teisę

67. Dėl būtinos teisėkūros priemonės rūšies Teisėsaugos direktyvos 33 konstatuojamojoje dalyje nurodyta, kad „kai šioje direktyvoje daroma nuoroda į valstybės narės teisę, teisinį pagrindą arba teisėkūros priemonę, tai nebūtinai reiškia, kad parlamentas turi priimti teisės aktą, nedarant poveikio reikalavimams, taikomiems pagal atitinkamos valstybės narės konstitucinę tvarką“[51].

68. Pagal Chartijos 52 straipsnio 1 dalį bet koks Chartijoje pripažintų teisių ir laisvių įgyvendinimo apribojimas turi būti „numatytas įstatymo“. Tai atspindi EŽTK 8 straipsnio 2 dalyje išreikštą mintį dėl teisių apribojimo, kuris teisėtas tik „įstatymų numatytais atvejais“, o tai reiškia ne tik taikytinų įstatymų laikymąsi, bet ir tokių įstatymų kokybę, pagal kurią jie turėtų būti suderinami su teisine valstybe, nedarant poveikio akto pobūdžiui.

69. Be to, Teisėsaugos direktyvos 33 konstatuojamojoje dalyje nurodyta: „[t]ačiau tokia valstybės narės teisė, teisinis pagrindas ar teisėkūros priemonė turėtų būti aiškūs ir tikslūs, o jų taikymas numatomas tiems subjektams, kuriems jie turi būti taikomi, kaip reikalaujama pagal Teisingumo Teismo ir Europos Žmogaus Teisių Teismo praktiką. Valstybės narės teisėje, kuria reglamentuojamas asmens duomenų tvarkymas šios direktyvos taikymo srityje, turėtų būti konkrečiai nurodyti bent siekiai, tvarkytini asmens duomenys, duomenų tvarkymo tikslai ir procedūros asmens duomenų vientisumui bei konfidencialumui užtikrinti, taip pat jų sunaikinimo procedūros.“

[49] Teisėsaugos direktyvos 3 straipsnio 13 punktas: „biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys“.

[50] WP258, nuomonė dėl kai kurių esminių Teisėsaugos direktyvos (Direktyvos (ES) 2016/680) aspektų, p. 7.

[51] Svarstomų teisėkūros priemonių rūšis turi atitikti ES teisę arba nacionalinę teisę. Priklausomai nuo apribojimo suvaržymo lygio, gali būti reikalaujama, kad, atsižvelgiant į normos lygį, nacionaliniu lygmeniu būtų priimta atitinkama teisėkūros priemonė.

70. Visų pirma, nacionaliniai įstatymai turėtų būti pakankamai aiškūs, kad suteiktų piliečiams pakankamai informacijos, kokiomis aplinkybėmis ir sąlygomis duomenų valdytojai turi teisę naudotis bet kokiomis tokiomis priemonėmis. Tai apima galimas išankstines duomenų tvarkymo sąlygas, pvz., konkrečias įrodymų rūšis, taip pat būtinybę gauti teismo ar vidaus leidimą. Atitinkami teisės aktai gali būti technologiškai neutralūs, jei tinkamai atsižvelgiama į konkrečią riziką ir ypatumus, susijusius su asmens duomenų tvarkymu veido atpažinimo technologijos sistemose. Remiantis Teisėsaugos direktyva ir Europos Sąjungos Teisingumo Teismo (ESTT) bei Europos Žmogaus Teisių Teismo (EŽTT) jurisprudencija, iš tiesų labai svarbu, kad teisėkūros priemonės, kuriomis veido atpažinimo priemonei siekiama suteikti teisinį pagrindą, duomenų subjektams būtų nuspėjamos.

71. Teisėkūros priemone negalima remtis kaip įstatymu, leidžiančiu tvarkyti biometrinius duomenis naudojant veido atpažinimo technologiją teisėsaugos tikslais, jeigu ja tik perkeliama Teisėsaugos direktyvos 10 straipsnio bendroji nuostata.

72. Be biometrinių duomenų, Teisėsaugos direktyvos 10 straipsnyje reglamentuojamas kitų specialių kategorijų duomenų, pavyzdžiui, seksualinės orientacijos, politinių nuomonių ir religinių įsitikinimų, tvarkymas, taigi jis apima platų duomenų tvarkymo spektrą. Be to, tokioje nuostatoje trūktų konkrečių reikalavimų, nurodančių aplinkybes ir sąlygas, kuriomis teisėsaugos institucijos būtų įgaliotos naudoti veido atpažinimo technologiją. Atsižvelgiant į nuorodą į kitų rūšių duomenis ir aiškų specialių apsaugos priemonių poreikį be papildomų patikslinimų, nacionalinės teisės nuostata, kuria į nacionalinę teisę perkeliamas Teisėsaugos direktyvos 10 straipsnis (su panašia bendra ir abstrakčia formuluote), negali būti naudojama kaip teisinis pagrindas tvarkyti biometrinius duomenis, susijusius su veido atpažinimu, nes ji būtų netiksli ir nenuspėjama. Pagal Teisėsaugos direktyvos 28 straipsnio 2 dalį arba 46 straipsnio 1 dalies c punktą, prieš teisės aktų leidėjui parengiant naują teisinį pagrindą bet kokios formos biometrinių duomenų tvarkymui naudojant veido atpažinimą, reikėtų pasikonsultuoti su nacionaline duomenų apsaugos priežiūros institucija.

3.2.1.2 Tikrai būtina

73. Duomenų tvarkymas gali būti laikomas „tikrai būtinu“ tik tuo atveju, jei asmens duomenų apsaugos suvaržymas ir jo apribojimai apsiriboja tik tuo, kas yra absoliučiai būtina[52]. Papildymas žodžiu „tikrai“ reiškia, kad teisės aktų leidėjas siekė, kad specialių kategorijų duomenys būtų tvarkomi tik dar griežtesnėmis sąlygomis nei būtinumo sąlygos (žr. 3.1.3.4 punktą). Šis reikalavimas turėtų būti aiškinamas kaip būtinas. Jis iki absoliutaus minimumo apriboja teisėsaugos institucijai suteikiamą vertinimo laisvę taikant būtinumo kriterijų. Remiantis suformuota Europos Sąjungos Teisingumo Teismo jurisprudencija, „tikro būtinumo“ sąlyga taip pat glaudžiai susijusi su objektyvių kriterijų reikalavimu, kad būtų galima apibrėžti aplinkybes ir sąlygas, kuriomis gali būti vykdomas duomenų tvarkymas, tokiu būdu užkertant kelią bet kokiam bendro ar sisteminio pobūdžio duomenų tvarkymui[53].

3.2.1.3 Akivaizdžiai paskelbta viešai

74. Vertinant, ar duomenų tvarkymas yra susijęs su duomenimis, kuriuos duomenų subjektas akivaizdžiai paskelbė viešai, reikėtų priminti, kad pati nuotrauka nėra sistemingai laikoma biometriniais

[52] Nuosekli jurisprudencija dėl pagrindinės teisės į pagarbą privačiam gyvenimui, žr. ESTT sprendimo byloje C-73/07 56 punktą (*Satakunnan Markkinapörssi ir Satamedia*); ESTT sprendimo bylose C-92/09 ir C-93/09 77 punktą (*Schecke ir Eifert*); ESTT sprendimo byloje C-594/12 52 punktą (*Skaitmeninės teisės*); ESTT sprendimo byloje C-362/14 92 punktą (*Schrems*).

[53] ESTT sprendimas byloje C-623/17, 78 punktas.

duomenimis[54]. Todėl tai, kad duomenų subjektas yra akivaizdžiai paskelbęs nuotrauką viešai, nereiškia, kad akivaizdžiai paskelbtais viešai laikomi ir su ja susiję biometriniai duomenys, kuriuos iš nuotraukos galima gauti specialiomis techninėmis priemonėmis.

75. Kalbant apie asmens duomenis apskritai, kad biometriniai duomenys būtų laikomi duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai, duomenų subjektas turi būti tyčia pateikęs biometrinių duomenų šabloną (o ne tiesiog veido atvaizdą), kuris būtų laisvai prieinamas ir skelbiamas atvirajame šaltinyje. Jei biometrinius duomenis atskleidžia trečioji šalis, negali būti laikoma, kad duomenų subjektas yra juos akivaizdžiai paskelbęs viešai.

76. Be to, nepakanka išaiškinti duomenų subjekto elgesį, kad būtų galima manyti, jog biometriniai duomenys buvo akivaizdžiai paskelbti viešai. Pavyzdžiui, socialinių tinklų ar interneto platformų atveju EDAV mano, kad to, kad duomenų subjektas nejjungė ar nenustatė konkrečių privatumo funkcijų, nepakanka, kad būtų galima laikyti, jog šis duomenų subjektas akivaizdžiai paskelbė savo asmens duomenis viešai ir kad šie duomenys (pvz., nuotraukos) gali būti tvarkomi kuriant biometrinių duomenų šablonus ir naudojami tapatybės nustatymo tikslais be duomenų subjekto sutikimo. Apskritai standartiniai paslaugos nustatymai, pvz., kad šablonus galima skelbti viešai, arba pasirinkimo nebuvimas, pvz., šablonai skelbiami viešai, o naudotojas šio nustatymo pakeisti negali, jokiu būdu neturėtų būti laikomi akivaizdžiai viešai paskelbtais duomenimis.

3.2.2 Automatizuotas individualių sprendimų priėmimas, įskaitant profiliavimą

77. Teisėsaugos direktyvos 11 straipsnio 1 dalyje numatyta valstybių narių pareiga apskritai uždrausti priimti sprendimus remiantis tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, dėl kurio duomenų subjektui kyla neigiamų teisinių pasekmių arba kuris turi jam didelės įtakos. Kaip šio bendro draudimo išimtis, toks duomenų tvarkymas gali būti įmanomas tik jeigu tai leidžiama pagal Sąjungos ar valstybės narės teisę, kuri taikoma duomenų valdytojui ir kuria nustatytos tinkamos duomenų subjekto teisių ir laisvių, bent teisės reikalauti iš duomenų valdytojo žmogaus įsikišimo, apsaugos priemonės. Jis gali būti taikomas tik ribotai. Ši riba taikoma įprastų (t. y. ne specialių) kategorijų asmens duomenims. Dar didesnė riba ir dar labiau apribotas naudojimas taikomas Teisėsaugos direktyvos 11 straipsnio 2 dalyje numatytai išimčiai. Joje dar kartą pabrėžiama, kad sprendimai pagal 1 dalį negali būti grindžiami specialių kategorijų asmens duomenimis, t. y. visų pirma biometriniais duomenimis, siekiant nustatyti unikalią fizinio asmens tapatybę. Išimtis gali būti numatyta tik tuo atveju, jei taikomos tinkamos priemonės duomenų subjekto teisėms ir laisvėms ir teisėtiems atitinkamo fizinio asmens interesams apsaugoti. Ši išimtis turi būti aiškinama kartu taikant Teisėsaugos direktyvos 10 straipsnio prielaidas ir į jas atsižvelgiant.

78. Priklausomai nuo veido atpažinimo technologijos sistemos, net žmogaus įsikišimas vertinant veido atpažinimo technologijos taikymo rezultatus nebūtinai savaime gali suteikti pakankamą garantiją, kad bus gerbiamos asmenų teisės, visų pirma teisė į asmens duomenų apsaugą, atsižvelgiant į galimą šališkumą ir klaidas, kurių gali atsirasti dėl paties duomenų tvarkymo. Be to, žmogaus įsikišimas gali būti laikomas apsaugos priemone tik tuo atveju, jei įsikišęs asmuo žmogaus įsikišimo metu gali kritiškai kvestionuoti veido atpažinimo technologijos taikymo rezultatus. Labai svarbu, kad asmuo galėtų suprasti veido atpažinimo technologijos sistemą ir jos ribas, taip pat tinkamai išaiškinti jos taikymo rezultatus. Taip pat būtina sukurti tokią darbo vietą ir organizaciją, kuri neutralizuotų automatizavimo

[54] Plg. BDAR 51 konstatuojamąją dalį: „Nuotraukų tvarkymas neturėtų būti sistemingai laikomas specialių kategorijų asmens duomenų tvarkymu, nes nuotraukoms biometrinių duomenų apibrėžtis taikoma tik tuo atveju, kai jos tvarkomos taikant specialias technines priemones, leidžiančias konkrečiai nustatyti fizinio asmens tapatybę ar tapatumą. “

šališkumo poveikį ir neskatintų nekritiško rezultatų priėmimo, pavyzdžiui, dėl laiko stokos, sudėtingų procedūrų, galimo žalingo poveikio karjerai ir kt.

79. Pagal Teisėsaugos direktyvos 11 straipsnio 3 dalį profiliavimas, sukeliantis fizinių asmenų diskriminaciją remiantis specialių kategorijų asmens duomenimis, pavyzdžiui, biometriniais duomenimis, draudžiamas pagal Sąjungos teisę. Pagal Teisėsaugos direktyvos 3 straipsnio 4 punktą profiliavimas – bet kokios formos automatizuotas asmens duomenų tvarkymas, kai asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti arba numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, vieta arba judėjimu. Svarstant, ar numatytos tinkamos priemonės atitinkamo fizinio asmens teisėms ir laisvėms bei teisėtiems interesams apsaugoti, reikia nepamiršti, kad naudojant veido atpažinimo technologiją gali būti taikomas profiliavimas, atsižvelgiant į tai, kaip ir kokiu tikslu ta technologija taikoma. Bet kuriuo atveju pagal Sąjungos teisę ir Teisėsaugos direktyvos 11 straipsnio 3 dalį profiliavimas, sukeliantis fizinių asmenų diskriminaciją remiantis specialių kategorijų asmens duomenimis, draudžiamas.

3.2.3 Duomenų subjektų kategorijos

80. Teisėsaugos direktyvos 6 straipsnyje kalbama apie būtinybę atskirti skirtingų kategorijų duomenų subjektus. Šis atskyrimas turi būti vykdomas, kai taikytina ir kiek įmanoma. Jis turi padaryti poveikį duomenų tvarkymo būdui. Iš Teisėsaugos direktyvos 6 straipsnyje pateiktų pavyzdžių galima daryti išvadą, kad paprastai asmens duomenų tvarkymas turi atitikti būtinumo ir proporcingumo kriterijus, taip pat atsižvelgiant į duomenų subjektų kategoriją[55]. Be to, galima daryti išvadą, kad kalbant apie duomenų subjektus, kurių atžvilgiu nėra įrodymų, kuriais remiantis būtų galima teigti, kad jų elgesys gali būti susijęs, net ir netiesiogiai ar nuotoliniu būdu, su teisėtu tikslu, kaip nustatyta Teisėsaugos direktyvoje, labiausiai tikėtina, kad suvaržymas nebus pagrįstas[56]. Jei pagal Teisėsaugos direktyvos 6 straipsnį atskyrimas netaikomas ir nėra įmanomas, vertinant suvaržymo būtinumą ir proporcingumą turi būti griežtai atsižvelgiama į Teisėsaugos direktyvos 6 straipsnio taisyklės išimtį. Skirtingų kategorijų duomenų subjektų atskyrimas yra esminis reikalavimas tvarkant asmens duomenis, kai tai susiję su veido atpažinimu, taip pat atsižvelgiant į galimus klaidingai teigiamus arba klaidingai neigiamus rezultatus, kurie gali turėti didelį poveikį duomenų subjektams ir tyrimo eigai.

81. Kaip minėta, įgyvendinant Sąjungos teisę, turi būti laikomasi Europos Sąjungos pagrindinių teisių chartijos nuostatų, plg. Chartijos 52 straipsnį. Todėl Teisėsaugos direktyvoje nustatytas pagrindas ir kriterijai turi būti aiškinami atsižvelgiant į Chartiją. ES ir jos valstybių narių teisės aktai negali būti mažiau griežti nei ši priemonė ir turi užtikrinti visapusišką Chartijos veiksmingumą.

3.2.4 Duomenų subjekto teisės

82. EDAV jau pateikė gaires dėl duomenų subjektų teisių pagal įvairius BDAR aspektus[57]. Teisėsaugos direktyvoje numatytos panašios duomenų subjektų teisės, o bendrosios gairės šiuo klausimu pateiktos 29 straipsnio darbo grupės nuomonėje, kuriai EDAV pritarė[58]. Tam tikromis aplinkybėmis Teisėsaugos direktyvoje numatyti tam tikri šių teisių apribojimai. Tokių apribojimų parametrai bus išsamiau pristatyti 3.2.4.6 skirsnyje „Teisėti duomenų subjekto teisių apribojimai“.

83. Nors visos Teisėsaugos direktyvos III skyriuje išvardytos duomenų subjekto teisės, savaime suprantama, taip pat taikomos asmens duomenų tvarkymui naudojant veido atpažinimo technologiją,

[55] Taip pat plg. ESTT sprendimo byloje C-594/12 56–59 punktus.
[56] Taip pat plg. ESTT sprendimo byloje C-594/12 58 punktą.
[57] Žr., pavyzdžiui, 2022 m. sausio 1 d. EDAV gaires 1/2022 dėl duomenų subjekto teisių – teisės susipažinti su duomenimis ir EDAV gaires 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus.
[58] WP258, nuomonė dėl kai kurių esminių Teisėsaugos direktyvos (Direktyvos (ES) 2016/680) aspektų.

kitame skyriuje daug dėmesio bus skiriama tam tikroms teisėms ir aspektams, dėl kurių gali būti itin svarbu pateikti rekomendacijų. Be to, šis skyrius ir jo analizė priklauso nuo to, ar atitinkamas duomenų tvarkymas naudojant veido atpažinimo technologiją atitinka ankstesniame skyriuje aprašytus teisinius reikalavimus.

84. Atsižvelgiant į asmens duomenų tvarkymo naudojant veido atpažinimo technologiją pobūdį (specialių kategorijų asmens duomenų tvarkymas dažnai nesant akivaizdžios sąveikos su duomenų subjektu), duomenų valdytojas, prieš pradėdamas duomenų tvarkymą naudojant veido atpažinimo technologiją, turi atidžiai apsvarstyti, kaip (arba ar įmanoma) įvykdyti Teisėsaugos direktyvos reikalavimus. Visų pirma atidžiai išnagrinėjama:

- kas yra duomenų subjektai (dažnai tai yra daugiau nei vienas subjektas, kuris yra pagrindinis duomenų tvarkymo objektas);
- kaip duomenų subjektai informuojami apie duomenų tvarkymą naudojant veido atpažinimo technologiją (žr. 3.2.4.1 skirsnį);
- kaip duomenų subjektai gali pasinaudoti savo teisėmis (šiuo atveju tiek informavimo ir prieigos teises, tiek teises, kad asmens duomenys būtų ištaisyti arba kad būtų apribotas jų naudojimas, gali būti ypač sudėtinga užtikrinti, jei veido atpažinimo technologija naudojama visiems patikrinimams, išskyrus patikrinimą „1 su 1“ tiesioginio kontakto su duomenų subjektu metu).

3.2.4.1 Teisių ir informacijos pateikimas duomenų subjektams glausta, suprantama ir lengvai prieinama forma

85. Veido atpažinimo technologijoje numatyti sunkumai, su kuriais susiduriama siekiant užtikrinti, kad duomenų subjektai būtų informuoti apie tai, kad jų biometriniai duomenys yra tvarkomi. Tai ypač sudėtinga, jei teisėsaugos institucija, naudodamasi veido atpažinimo technologija, analizuoja iš trečiosios šalies gautą arba trečiosios šalies pateiktą vaizdo medžiagą, nes teisėsaugos institucija turi mažai, o dažniausiai visai neturi galimybių informuoti duomenų subjektą tuo metu, kai duomenys surenkami (pvz., įrengiant ženklą vietoje). Prieš pradedant bet kokį biometrinių duomenų tvarkymą, bet kokia vaizdo medžiaga, nesusijusi su tyrimu (arba duomenų tvarkymo tikslu), visada turėtų būti pašalinama arba nuasmeninama (pvz., užtušuojant ir nesuteikiant galimybės atkurti duomenis), kad būtų išvengta pavojaus, kad nebus įvykdytas Teisėsaugos direktyvos 4 straipsnio 1 dalies e punkte nustatytas duomenų kiekio mažinimo principas ir tos direktyvos 13 straipsnio 2 dalyje nustatytos informavimo pareigos. Duomenų valdytojas privalo įvertinti, kokia informacija būtų svarbi duomenų subjektui naudojantis savo teisėmis, ir užtikrinti, kad būtina informacija būtų pateikta. Veiksmingas duomenų subjekto teisių įgyvendinimas priklauso nuo to, ar duomenų valdytojas vykdo savo informavimo pareigas.

86. Teisėsaugos direktyvos 13 straipsnio 1 dalyje nustatyta, kokia būtiniausia informacija apskritai turi būti teikiama duomenų subjektui. Ši informacija gali būti pateikiama duomenų valdytojo svetainėje, spausdintine forma (pvz., paprašius pateikiamas lankstinukas) arba kitais duomenų subjektui lengvai prieinamais būdais. Bet kuriuo atveju duomenų valdytojas privalo užtikrinti, kad būtų veiksmingai pateikta informacija, susijusi bent su šiais elementais:

- duomenų valdytojo, įskaitant duomenų apsaugos pareigūną, tapatybe ir kontaktiniais duomenimis,
- duomenų tvarkymo tikslu ir tuo, kad duomenys tvarkomi naudojant veido atpažinimo technologiją,
- teise pateikti skundą priežiūros institucijai ir tokios institucijos kontaktiniais duomenimis;

- teise prašyti suteikti prieigą prie asmens duomenų, juos ištaisyti ar ištrinti, taip pat apriboti asmens duomenų tvarkymą.

87. Be to, konkrečiais nacionalinėje teisėje apibrėžtais atvejais, kurie turėtų atitikti Teisėsaugos direktyvos 13 straipsnio 2 dalį[59], pavyzdžiui, kai duomenys tvarkomi naudojant veido atpažinimo technologiją, duomenų subjektui turi būti tiesiogiai pateikta ši informacija:

- duomenų tvarkymo teisiniu pagrindu,
- informaciją apie tai, kur asmens duomenys buvo surinkti be duomenų subjekto žinios,
- laikotarpiu, kurį asmens duomenys bus saugomi, arba, jei tai neįmanoma, kriterijais, pagal kuriuos tas laikotarpis nustatomas,
- jei taikytina, asmens duomenų gavėjų kategorijomis (įskaitant trečiąsias valstybes arba tarptautines organizacijas).

88. Nors Teisėsaugos direktyvos 13 straipsnio 1 dalyje kalbama apie visuomenei teikiamą bendrą informaciją, tos direktyvos 13 straipsnio 2 dalyje kalbama apie papildomą informaciją, kuri turi būti pateikta konkrečiam duomenų subjektui konkrečiais atvejais, pavyzdžiui, kai duomenys renkami tiesiogiai iš duomenų subjekto arba netiesiogiai be duomenų subjekto žinios[60]. Nėra aiškios apibrėžties, ką reiškia 13 straipsnio 2 dalyje vartojama sąvoka „konkretūs atvejai“. Tačiau ji taikoma tais atvejais, kai duomenų subjektai turi būti informuoti apie konkrečiai su jais susijusį duomenų tvarkymą ir jiems turi būti suteikta tinkama informacija, kad jie galėtų veiksmingai naudotis savo teisėmis. EDAV mano, kad vertinant, ar yra „konkretus atvejis“, reikia atsižvelgti į keletą veiksnių, įskaitant tai, ar asmens duomenys renkami be duomenų subjekto žinios, nes tai būtų vienintelis būdas suteikti duomenų subjektams galimybę veiksmingai naudotis savo teisėmis. Kiti „konkrečių atvejų“ pavyzdžiai galėtų būti atvejai, kai asmens duomenys toliau tvarkomi pagal tarptautinio bendradarbiavimo baudžiamosiose bylose procedūrą arba kai asmens duomenys tvarkomi vykdant slaptas operacijas, kaip nurodyta nacionalinėje teisėje. Be to, iš Teisėsaugos direktyvos 38 konstatuojamosios dalies matyti, kad jeigu sprendimai priimami remiantis tik veido atpažinimo technologija, duomenų subjektai turi būti informuojami apie automatizuoto sprendimų priėmimo ypatybes. Tai taip pat rodytų, kad yra susiklostęs konkretus atvejis, kai pagal Teisėsaugos direktyvos 13 straipsnio 2 dalį duomenų subjektui turėtų būti pateikta papildoma informacija[61].

89. Galiausiai reikėtų pažymėti, kad pagal Teisėsaugos direktyvos 13 straipsnio 3 dalį valstybės narės gali priimti teisėkūros priemones, kuriomis tam tikrais atvejais, siekiant tam tikrų tikslų, pareiga teikti informaciją apribojama. Tai taikoma tiek, kiek ir tol, kol tokia priemonė yra demokratinėje visuomenėje būtina ir proporcinga priemonė, tinkamai atsižvelgiant į duomenų subjekto pagrindines teises ir teisėtus interesus.

3.2.4.2 Teisė susipažinti su duomenimis

90. Apskritai duomenų subjektas turi teisę gauti teigiamą arba neigiamą patvirtinimą apie bet kokį jo asmens duomenų tvarkymą ir, jei atsakymas teigiamas, galimybę susipažinti su pačiais asmens duomenimis bei papildomos informacijos, kaip nurodyta Teisėsaugos direktyvos 14 straipsnyje. Veido

[59] Pvz., Vokietijos federalinio duomenų apsaugos įstatymo 56 straipsnio 1 dalis, kurioje, be kita ko, nurodyta, kokią informaciją reikia pateikti duomenų subjektams vykdant slaptas operacijas.
[60] WP258, nuomonė dėl kai kurių esminių Teisėsaugos direktyvos (Direktyvos (ES) 2016/680) aspektų, p. 17–18.
[61] Atkreiptinas dėmesys į skirtumą tarp Teisėsaugos direktyvos 13 straipsnio 1 dalyje vartojamos sąvokos „padaryti prieinama duomenų subjektui“ ir tos direktyvos 13 straipsnio 2 dalyje vartojamos sąvokos „pateikti duomenų subjektui“. Pagal Teisėsaugos direktyvos 13 straipsnio 2 dalį duomenų valdytojas turi užtikrinti, kad informacija pasiektų duomenų subjektą, jei svetainėje paskelbtos informacijos nepakaks.

atpažinimo technologijos atveju, kai biometriniai duomenys saugomi ir su tapatybe susieti taip pat raidiniais skaitmeniniais duomenimis, tai turėtų leisti kompetentingai institucijai patvirtinti prašymą leisti susipažinti su duomenimis remiantis paieška pagal tuos raidinius skaitmeninius duomenis ir nepradedant jokio tolesnio kitų asmenų biometrinių duomenų tvarkymo (t. y. paieškos duomenų bazėje naudojant veido atpažinimo technologiją). Turi būti laikomasi duomenų kiekio mažinimo principo ir turėtų būti saugoma ne daugiau duomenų nei būtina atsižvelgiant į duomenų tvarkymo tikslą.

3.2.4.3 Teisė ištaisyti asmens duomenis

91. Kadangi veido atpažinimo technologija nenumato absoliutaus tikslumo, ypač svarbu, kad duomenų valdytojai atidžiai reaguotų į prašymus ištaisyti asmens duomenis. Taip gali būti ir tuo atveju, kai remiantis veido atpažinimo technologija duomenų subjektas buvo netiksliai priskirtas prie kategorijos, pvz., neteisingai priskirtas įtariamųjų kategorijai, remiantis pradine prielaida dėl veiksmų eigos vaizdo medžiagoje. Pavojus duomenų subjektams yra ypač didelis, jeigu tokie netikslūs duomenys saugomi policijos duomenų bazėje ir (arba) jais dalijamasi su kitais subjektais. Duomenų valdytojas privalo atitinkamai ištaisyti saugomus duomenis ir veido atpažinimo technologijos sistemas, žr. Teisėsaugos direktyvos 47 konstatuojamąją dalį.

3.2.4.4 Teisė reikalauti ištrinti duomenis

92. Veido atpažinimo technologija daugeliu atvejų, jei ji nėra naudojama patikrinimui „1 su 1“ ir (arba) tapatybės patvirtinimui, prilygs daugelio duomenų subjektų biometrinių duomenų tvarkymui. Todėl svarbu, kad duomenų valdytojas iš anksto apsvarstytų, kur yra jo tikslo ir būtinumo ribos, kad prašymą ištrinti duomenis pagal 16 straipsnį būtų galima išnagrinėti nepagrįstai nedelsiant (nes duomenų valdytojas, be kita ko, turi ištrinti asmens duomenis, kurie yra tvarkomi daugiau, nei leidžiama pagal taikytinus teisės aktus, remiantis Teisėsaugos direktyvos 4, 8 ir 10 straipsniais).

3.2.4.5 Teisė apriboti duomenų tvarkymą

93. Jeigu duomenų subjektas ginčija duomenų tikslumą, o duomenų tikslumo negalima patvirtinti (arba kai asmens duomenys turi būti saugomi būsimų įrodymų tikslais), duomenų valdytojas privalo apriboti to duomenų subjekto asmens duomenis pagal Teisėsaugos direktyvos 16 straipsnį. Tai ypač svarbu, kai kalbama apie veido atpažinimo technologiją (pagrįstą algoritmu (-ais) ir todėl niekada nerodančią galutinio rezultato), kai surenkama daug duomenų ir atpažinimo tikslumas bei kokybė gali skirtis. Dėl prastos kokybės vaizdo medžiagos (pvz., nusikaltimo vietoje) didėja klaidingų teigiamų rezultatų rizika. Be to, jei stebėjimo sąraše esantys veido atvaizdai nėra reguliariai atnaujinami, taip pat padidėja klaidingų teigiamų arba klaidingų neigiamų rezultatų rizika. Konkrečiais atvejais, kai duomenų negalima ištrinti dėl to, kad yra pagrįstų priežasčių manyti, jog ištrynimas galėtų paveikti duomenų subjekto teisėtus interesus, duomenys turėtų būti ribojami ir tvarkomi tik tuo tikslu, dėl kurio jie negalėjo būti ištrinti (žr. Teisėsaugos direktyvos 47 konstatuojamąją dalį).

3.2.4.6 Teisėti duomenų subjekto teisių apribojimai

94. Kalbant apie duomenų valdytojo pareigas teikti informaciją ir duomenų subjektų teisę susipažinti su duomenimis, apribojimai leidžiami tik tiek, kiek jie nustatyti įstatyme, ir tai savo ruožtu turi būti būtina ir proporcinga demokratinės visuomenės priemonė, tinkamai atsižvelgiant į atitinkamo fizinio asmens pagrindines teises ir teisėtus interesus (žr. Teisėsaugos direktyvos 13 straipsnio 3 dalį, 13 straipsnio 4 dalį, 15 straipsnį ir 16 straipsnio 4 dalį). Kai veido atpažinimo technologija naudojama teisėsaugos tikslais, galima tikėtis, kad ji bus naudojama tokiomis aplinkybėmis, kai tai kenktų siekiamam tikslui informuoti duomenų subjektą arba leisti susipažinti su duomenimis. Tai būtų taikoma, pavyzdžiui, policijos atliekamam nusikaltimo tyrimui arba siekiant užtikrinti nacionalinį saugumą ar visuomenės saugumą.

95. Teisė susipažinti su informacija nereiškia automatinės prieigos prie visos informacijos, pvz., baudžiamojoje byloje, kurioje tvarkomi asmens duomenys. Svarbus pavyzdys, kada gali būti leidžiami teisės apribojimai, galėtų būti nusikalstamos veikos tyrimas.

3.2.4.7 Naudojimasis teisėmis per priežiūros instituciją

96. Tais atvejais, kai taikomi teisėti teisių įgyvendinimo apribojimai pagal Teisėsaugos direktyvos III skyrių, duomenų subjektas gali prašyti duomenų apsaugos institucijos įgyvendinti savo teises jo vardu patikrinant duomenų valdytojo atliekamo duomenų tvarkymo teisėtumą. Duomenų valdytojas privalo informuoti duomenų subjektą apie galimybę tokiu būdu pasinaudoti savo teisėmis (žr. Teisėsaugos direktyvos 17 straipsnį ir 46 straipsnio 1 dalies g punktą). Veido atpažinimo technologijos atveju tai reiškia, kad duomenų valdytojas turi užtikrinti, kad būtų įdiegtos tinkamos priemonės, kad toks prašymas galėtų būti išnagrinėtas, pavyzdžiui, kad būtų galima atlikti įrašytos medžiagos paiešką, jei duomenų subjektas pateikia pakankamai informacijos, kad būtų galima rasti jo asmens duomenis.

3.2.5 Kiti teisiniai reikalavimai ir apsaugos priemonės

3.2.5.1 27 straipsnis „Poveikio duomenų apsaugai vertinimas“

97. Poveikio duomenų apsaugai vertinimas (PDAV) prieš pradedant naudoti veido atpažinimo technologiją yra privalomas reikalavimas, nes toks duomenų tvarkymas, visų pirma naudojant naujas technologijas ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms. Atsižvelgiant į tai, kad veido atpažinimo technologijos naudojimas apima sistemingą automatinį specialių kategorijų duomenų tvarkymą, galima daryti prielaidą, kad tokiais atvejais duomenų valdytojas paprastai privalėtų atlikti PDAV. PDAV turėtų būti pateiktas bent bendras numatytų duomenų tvarkymo operacijų aprašymas, duomenų tvarkymo operacijų būtinumo ir proporcingumo, palyginti su tikslais, įvertinimas, pavojaus duomenų subjektų teisėms ir laisvėms įvertinimas, numatytos priemonės tam pavojui pašalinti, apsaugos priemonės, saugumo priemonės ir mechanizmai, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi reikalavimų. EDAV rekomenduoja paviešinti tokių vertinimų rezultatus arba bent pagrindinius PDAV nustatytus faktus ir išvadas, kaip pasitikėjimo ir skaidrumo didinimo priemonę[62].

3.2.5.2 28 straipsnis „Išankstinis konsultavimasis su priežiūros institucija“

98. Pagal Teisėsaugos direktyvos 28 straipsnį duomenų valdytojas arba duomenų tvarkytojas, prieš pradėdamas tvarkyti duomenis, turi konsultuotis su priežiūros institucija, jeigu: a) poveikio duomenų apsaugai vertinime nurodyta, kad atliekant duomenų tvarkymą kiltų didelis pavojus tuo atveju, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, arba b) dėl duomenų tvarkymo rūšies, visų pirma naudojant naujas technologijas, mechanizmus ar taikant naujas procedūras, kyla didelis pavojus duomenų subjektų teisėms ir laisvėms. Kaip jau paaiškinta šių gairių 2.3 skirsnyje, EDAV mano, kad dauguma veido atpažinimo technologijos diegimo ir naudojimo atvejų iš esmės kelia didelį pavojų duomenų subjektų teisėms ir laisvėms. Todėl, be PDAV, veido atpažinimo technologiją taikanti institucija prieš pradėdama naudoti šią sistemą turėtų konsultuotis su kompetentinga priežiūros institucija.

3.2.5.3 29 straipsnis „Duomenų tvarkymo saugumas“

99. Dėl unikalaus biometrinių duomenų pobūdžio duomenų subjektas negali jų pakeisti, jei jie būtų neteisėtai atskleisti, pvz., dėl duomenų saugumo pažeidimo. Todėl veido atpažinimo technologiją įgyvendinanti ir (arba) naudojanti kompetentinga institucija turėtų skirti ypatingą dėmesį duomenų tvarkymo saugumui pagal Teisėsaugos direktyvos 29 straipsnį. Visų pirma teisėsaugos institucija turėtų užtikrinti, kad sistema atitiktų atitinkamus standartus, ir įgyvendinti biometrinių duomenų šablonų

[62] Daugiau informacijos rasite Poveikio duomenų apsaugai vertinimo (PDAV) gairėse kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, WP248, 1-oji peržiūrėta versija.

apsaugos priemones[63]. Ši pareiga yra dar svarbesnė, jei teisėsaugos institucija naudojasi trečiosios šalies paslaugų teikėjo (duomenų tvarkytojo) paslaugomis.

3.2.5.4 20 straipsnis „Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga“

100. Pritaikytosios ir standartizuotosios duomenų apsaugos pagal Teisėsaugos direktyvos 20 straipsnį tikslas – užtikrinti, kad duomenų apsaugos principai ir apsaugos priemonės, pavyzdžiui, duomenų kiekio mažinimas ir saugojimo apribojimai, būtų integruoti į technologiją taikant tinkamas technines ir organizacines priemones, pavyzdžiui, pseudonimų suteikimą, dar prieš pradedant tvarkyti asmens duomenis ir būtų taikomi visą jos gyvavimo ciklą. Atsižvelgiant į fizinių asmenų teisėms ir laisvėms būdingą didelę riziką, tokių priemonių pasirinkimas neturėtų priklausyti vien tik nuo ekonominių aplinkybių[64], o veikiau turėtų būti siekiama įgyvendinti pažangiausias duomenų apsaugos technologijas. Be to, jeigu teisėsaugos institucija ketina taikyti ir naudoti išorės teikėjų veido atpažinimo technologiją, ji turi užtikrinti, pavyzdžiui, vykdydama viešųjų pirkimų procedūrą, kad būtų naudojama tik veido atpažinimo technologija, sukurta remiantis pritaikytosios ir standartizuotosios duomenų apsaugos principais[65]. Tai taip pat reiškia, kad veido atpažinimo technologijos veikimo skaidrumas neribojamas reikalavimais dėl komercinių paslapčių ar intelektinės nuosavybės teisių.

3.2.5.5 25 straipsnis „Registravimas“

101. Teisėsaugos direktyvoje nustatyti įvairūs metodai, kaip duomenų valdytojas arba duomenų tvarkytojas įrodo duomenų tvarkymo teisėtumą ir užtikrina duomenų vientisumą bei duomenų saugumą. Šiuo atžvilgiu sistemos įrašai yra labai naudingas įrankis ir svarbi apsaugos priemonė, leidžianti patikrinti duomenų tvarkymo teisėtumą tiek viduje (t. y. savikontrolė), tiek išorės priežiūros institucijoms, pvz., duomenų apsaugos institucijoms. Pagal Teisėsaugos direktyvos 25 straipsnį automatizuoto duomenų tvarkymo sistemose turėtų būti saugomi registracijos įrašai bent apie šias duomenų tvarkymo operacijas: duomenų rinkimą, keitimą, susipažinimą su duomenimis, jų atskleidimą, įskaitant perdavimus, sujungimą ir ištrynimą. Be to, susipažinimo su duomenimis ir jų atskleidimo registracijos įrašais turėtų būti įmanoma nustatyti tokių operacijų pagrindimą, datą ir laiką ir, kiek įmanoma, asmens, kuris susipažino su asmens duomenimis arba juos atskleidė, tapatybę ir tokių asmens duomenų gavėjų tapatybę. Be to, naudojant veido atpažinimo sistemas, rekomenduojama registruoti šias papildomas duomenų tvarkymo operacijas (iš dalies viršijant Teisėsaugos direktyvos 25 straipsnį):

- etaloninės duomenų bazės pakeitimus (papildymą, ištrynimą ar atnaujinimą). Registracijos įraše turėtų būti saugoma atitinkamo (pridėto, ištrinto arba atnaujinto) atvaizdo kopija, kai duomenų tvarkymo operacijų teisėtumo ar rezultatų kitaip patikrinti neįmanoma;

- tapatybės nustatymo arba tikrinimo bandymus, įskaitant rezultatus ir patikimumo įvertinimą. Turėtų būti taikomas griežtas duomenų kiekio mažinimo principas, kad registracijos įrašuose būtų laikomas tik atvaizdo identifikatorius iš etaloninės duomenų bazės, užuot įrašant etaloninį atvaizdą. Reikėtų vengti registruoti įvestus biometrinius duomenis, nebent tai būtina (pvz., tik atitikties atvejais);

- naudotojo, kuris paprašė tapatybės nustatymo arba patikrinimo bandymo, tapatybės duomenis;

[63] Žr., pavyzdžiui, ISO/IEC 24745 Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Biometrinės informacijos apsauga.

[64] Žr. Teisėsaugos direktyvos 53 konstatuojamąją dalį.

[65] Išsamiau žr. EDAV pritaikytosios ir standartizuotosios duomenų apsaugos gaires, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

- sistemų įrašuose saugomiems asmens duomenims taikomi griežti tikslo apribojimai (pvz., auditas) ir jie neturėtų būti naudojami kitais tikslais (pvz., kad vis dar būtų galima atlikti atpažinimą ir (arba) patikrinimą, įskaitant atvaizdą, kuris buvo ištrintas iš etaloninių duomenų bazių). Siekiant užtikrinti įrašų vientisumą, turėtų būti taikomos saugumo priemonės, taip pat labai rekomenduojamos automatinės stebėsenos sistemos, skirtos nustatyti piktnaudžiavimą registracijos įrašais. Kalbant apie etaloninės duomenų bazės įrašus, veido atvaizdų saugojimo atveju saugumo priemonės turėtų būti lygiavertės etaloninei duomenų bazei. Be to, turėtų būti įdiegti automatiniai procesai, užtikrinantys įrašų duomenų saugojimo laikotarpio laikymąsi.

3.2.5.6 4 straipsnio 4 dalis. Atskaitomybė

102. Duomenų valdytojas turi galėti įrodyti, kad duomenų tvarkymas atitinka Teisėsaugos direktyvos 4 straipsnio 1–3 dalyse nustatytus principus, plg. Teisėsaugos direktyvos 4 straipsnio 4 dalį. Šiuo atžvilgiu labai svarbūs sistemingas ir aktualus sistemos dokumentavimas (įskaitant atnaujinimus, modernizavimą ir algoritminį mokymą), techninės ir organizacinės priemonės (įskaitant sistemos veikimo stebėseną ir galimą žmogaus įsikišimą) ir asmens duomenų tvarkymas. Siekiant įrodyti duomenų tvarkymo teisėtumą, ypač svarbus elementas yra registravimas pagal Teisėsaugos direktyvos 25 straipsnį (plg. 3.2.5.5 skirsnį). Atskaitomybės principas susijęs ne tik su sistema ir duomenų tvarkymu, bet ir su procedūrinių apsaugos priemonių, tokių kaip būtinumo ir proporcingumo vertinimai, poveikio duomenų apsaugai vertinimai, taip pat vidaus konsultacijos (pvz., projekto vadovų patvirtinimas arba vidaus sprendimai dėl patikimumo įvertinimo verčių) ir išorės konsultacijos (pvz., duomenų apsaugos institucija), dokumentavimu. II priede šiuo požiūriu pateikiama keletas elementų.

3.2.5.7 47 straipsnis. Veiksminga priežiūra

103. Veiksminga kompetentingų duomenų apsaugos institucijų vykdoma priežiūra yra viena iš svarbiausių asmenų, kuriems taikoma veido atpažinimo technologija, pagrindinių teisių ir laisvių apsaugos priemonių. Tuo pat metu būtina suteikti kiekvienai duomenų apsaugos institucijai būtinus žmogiškuosius, techninius ir finansinius išteklius, patalpas ir infrastruktūrą, kad jos galėtų veiksmingai vykdyti savo užduotis ir naudotis savo įgaliojimais[66]. Dar svarbiau nei turimų darbuotojų skaičius yra ekspertų įgūdžiai, kurie turėtų apimti labai platų klausimų spektrą – nuo baudžiamųjų tyrimų ir policijos bendradarbiavimo iki didžiųjų duomenų analizės ir dirbtinio intelekto. Todėl valstybės narės turėtų užtikrinti, kad priežiūros institucijų ištekliai būtų tinkami ir pakankami, kad jos galėtų vykdyti savo įgaliojimus apsaugoti duomenų subjektų teises, ir atidžiai stebėti visus pokyčius šioje srityje[67].

4 IŠVADA

104. Veido atpažinimo technologijų naudojimas yra iš esmės susijęs su didelio kiekio asmens duomenų, įskaitant specialių kategorijų duomenis, tvarkymu. Veidas ir apskritai biometriniai duomenys yra nuolat ir neatšaukiamai susieti su asmens tapatybe. Todėl veido atpažinimo naudojimas daro tiesioginį ar netiesioginį poveikį daugeliui ES pagrindinių teisių chartijoje įtvirtintų pagrindinių teisių ir laisvių, kurios gali būti susijusios ne tik su privačiu gyvenimu ir duomenų apsauga, pavyzdžiui, žmogaus orumui, judėjimo laisvei, susirinkimų laisvei ir kt. Tai ypač svarbu teisėsaugos ir baudžiamosios teisenos srityje.

[66] Žr. Komisijos komunikatą „Pirmoji Duomenų apsaugos teisėsaugos srityje direktyvos (ES) 2016/680 (Teisėsaugos direktyvos) taikymo ir veikimo ataskaita“, COM(2022) 364 *final*, 3.4.1 skirsnis.

[67] Žr. EDAV indėlio į Europos Komisijos atliktą Duomenų apsaugos teisėsaugos srityje direktyvos (Teisėsaugos direktyvos) vertinimą pagal 62 straipsnį, 14 punktą, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

105. EDAV supranta, jog teisėsaugos institucijoms reikia naudotis geriausiomis turimomis priemonėmis nustatant teroro aktų ir kitų sunkių nusikaltimų kaltininkus. Tačiau tokios priemonės turėtų būti naudojamos griežtai laikantis taikomos teisinės sistemos ir tik tais atvejais, kai jos atitinka būtinumo ir proporcingumo reikalavimus, kaip nustatyta Chartijos 52 straipsnio 1 dalyje. Be to, nors šiuolaikinės technologijos gali būti viena iš sprendimo dalių, jos jokiu būdu nėra stebuklingas sprendimas.

106. Esama tam tikrų veido atpažinimo technologijų naudojimo atvejų, dėl kurių asmenims ir visuomenei kyla nepriimtinai didelių pavojų (vadinamosios raudonosios linijos). Dėl šių priežasčių EDAV ir EDAPP paragino juos apskritai uždrausti[68].

107. Visų pirma nuotolinis biometriniais duomenimis pagrįstas asmenų tapatybės nustatymas viešai prieinamose erdvėse kelia didelį pavojų, kad bus kišamasi į privatų asmenų gyvenimą, ir jam nėra vietos demokratinėje visuomenėje, nes dėl savo pobūdžio jis susijęs su masiniu stebėjimu. Be to, EDAV mano, kad DI grindžiamos veido atpažinimo sistemos, kuriose asmenys pagal biometrinius duomenis skirstomi į grupes pagal etninę kilmę, lytį, taip pat politinę ar seksualinę orientaciją, yra nesuderinamos su Chartija. Be to, EDAV yra įsitikinusi, kad veido atpažinimo ar panašių technologijų naudojimas siekiant nustatyti fizinio asmens emocijas yra labai nepageidautinas ir turėtų būti uždraustas, galbūt numatant kelias tinkamai pagrįstas išimtis. Be to, EDAV mano, kad asmens duomenų tvarkymas teisėsaugos srityje, kuris būtų grindžiamas duomenų baze, užpildyta renkant asmens duomenis plačiu mastu ir nesirenkamai, pvz., perimant internete prieinamas nuotraukas ir veido atvaizdus, visų pirma tuos, kurie pateikiami socialiniuose tinkluose, iš esmės neatitiktų Sąjungos teisėje nustatyto tikro būtinumo reikalavimo.

5 PRIEDAI

I priedas. Pagalbinis modelis

II priedas. Praktinės rekomendacijos, kaip valdyti veido atpažinimo technologija grindžiamus projektus teisėsaugos institucijose

III priedas. Praktiniai pavyzdžiai

[68] Žr. EDAV ir EDAPP bendrą nuomonę 5/2021 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas)https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

I PRIEDAS. SCENARIJŲ APRAŠYMO ŠABLONAS

(su informacijos langeliais, skirtais scenarijuje nagrinėjamiems aspektams)

Duomenų tvarkymo aprašymas:

- Duomenų tvarkymo aprašymas, kontekstas (ryšys su nusikaltimu), tikslas

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☐ visi piliečiai ☐ nuteistieji ☐ įtariamieji ☐ vaikai ☐ kiti pažeidžiami duomenų subjektai
- Atvaizdo šaltinis: ☐ viešai prieinamos erdvės ☐ internetas ☐ privatus subjektas ☐ kiti asmenys ☐ kita .....
- Ryšys su nusikaltimu: ☐ Tiesioginis laikinis ☐ Netiesioginis laikinis ☐ Tiesioginis geografinis ☐ Netiesioginis geografinis ☐ Nebūtinas
- Informacijos užfiksavimo būdas: ☐ nuotolinis ☐ kabinoje arba kontroliuojamoje aplinkoje
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms:
  ☐ Ne
  Taip, būtent ☐ susirinkimų laisvei
  ☐ žodžio laisvei
  ☐ įvairioms:.....
- Galimi papildomi informacijos apie duomenų subjektą šaltiniai:
  ☐ asmens tapatybės dokumentas ☐viešojo telefono naudojimas ☐ transporto priemonės valstybinio numerio ženklas
  ☐ kita .....

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☐ bendrosios paskirties duomenų bazės ☐ specialios paskirties duomenų bazės, susijusios su nusikaltimo sritimi
- Aprašymas, kaip šios etaloninės duomenų bazės pildomos (ir teisinis pagrindas)
- Duomenų bazės paskirties keitimas (pvz., pagrindinis tikslas buvo privačiosios nuosavybės apsauga): ☐ TAIP ☐ NE

Algoritmas:

- Duomenų tvarkymo rūšis: ☐ patikrinimas „1 su 1“ (tapatybės patvirtinimas)☐ tapatybės nustatymas palyginant „1 su daugeliu“
- Tikslumo aspektai
- Techninės apsaugos priemonės

Rezultatai:

- Poveikis ☐ Tiesioginis (pvz., duomenų subjektas gali būti suimtas, apklaustas, diskriminacinis elgesys)

  ☐ Netiesioginis (naudojama statistiniams modeliams, nėra rimtų teisinių veiksmų prieš duomenų subjektus)

- Automatizuotas sprendimas: ☐ TAIP ☐ NE
- Saugojimo trukmė

<u>Teisinė analizė:</u>

- Būtinumo ir proporcingumo analizė – tikslas / nusikaltimo sunkumas / nesusijusių, bet su duomenų tvarkymo paveiktų asmenų skaičius
- Duomenų subjektui teikiamos išankstinės informacijos rūšis: ☐ Atvykstant į konkrečią zoną

  ☐ Teisėsaugos institucijos svetainėje apskritai

  ☐ Teisėsaugos institucijos svetainėje, skirtoje konkrečiam duomenų tvarkymui

  ☐ Kita .....
- Taikytina teisinė sistema:

  ☐ Teisėsaugos direktyva daugiausia perkelta į nacionalinę teisę

  ☐ Bendrojo pobūdžio nacionalinės teisės aktai dėl biometrinių duomenų naudojimo teisėsaugos institucijose

  ☐ Tos kompetentingos institucijos tokio duomenų tvarkymo (veido atpažinimas) specialieji nacionalinės teisės aktai

  ☐ Specialieji nacionalinės teisės aktai dėl tokio duomenų tvarkymo (automatizuotas sprendimas)

<u>Išvada:</u>

Bendrosios pastabos dėl to, ar aprašytas duomenų tvarkymas gali būti suderinamas su ES teise (ir kai kurie patarimai dėl teisinių išankstinių sąlygų)

II PRIEDAS. PRAKTINĖS REKOMENDACIJOS, KAIP VALDYTI VEIDO ATPAŽINIMO TECHNOLOGIJA GRINDŽIAMUS PROJEKTUS TEISĖSAUGOS INSTITUCIJOSE

Šiame priede pateikiamos papildomos praktinės rekomendacijos teisėsaugos institucijoms, planuojančioms pradėti projektą, susijusį su veido atpažinimo technologija. Jame pateikiama daugiau informacijos apie organizacines ir technines priemones, į kurias reikia atsižvelgti įgyvendinant projektą, ir jis neturėtų būti laikomas išsamiu veiksmų ir (arba) priemonių, kurių reikia imtis, sąrašu. Jis taip pat turėtų būti taikomas kartu su EDAV gairėmis 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus[69] ir bet kokiu ES ir EEE reglamentu bei EDAV gairėmis dėl dirbtinio intelekto naudojimo.

Šiame priede pateikiamos gairės, grindžiamos prielaida, kad teisėsaugos institucijos pirks veido atpažinimo technologiją (kaip standartinius produktus). Jei teisėsaugos institucija planuoja parengti (toliau mokyti) veido atpažinimo technologiją, taikomi papildomi reikalavimai renkantis būtinus mokymo, patvirtinimo ir bandymo duomenų rinkinius, kurie bus naudojami kūrimo metu, ir su vystymo aplinka susijusias funkcijas ir (arba) priemones. Panašiai, standartinį produktą gali prireikti papildomai pritaikyti atsižvelgiant į numatomą paskirtį; tokiu atveju turėtų būti laikomasi pirmiau minėtų bandymo, patvirtinimo ir mokymo duomenų rinkinių atrankos reikalavimų.

Priklausymas tai pačiai teisėsaugos institucijai savaime nesuteikia visapusiškos prieigos prie biometrinių duomenų. Kaip ir bet kurios kitos asmens duomenų kategorijos, biometriniai duomenys, surinkti tam tikru teisėsaugos tikslu pagal konkretų teisinį pagrindą, negali būti naudojami be tinkamo teisinio pagrindo kitu teisėsaugos tikslu (Direktyvos (ES) 2016/680 (Teisėsaugos direktyvos) 4 straipsnio 2 dalis). Be to, veido atpažinimo technologijos priemonės kūrimas ir (arba) mokymas laikomas kitu tikslu ir turėtų būti įvertinta, ar biometrinių duomenų tvarkymas siekiant įvertinti technologijos veiksmingumą ir (arba) ją apmokyti, siekiant išvengti neigiamo poveikio duomenų subjektams, susijusio su menku veiksmingumu, yra būtinas ir proporcingas atsižvelgiant į pradinį duomenų tvarkymo tikslą.

1. FUNKCIJOS IR PAREIGOS

Kai teisėsaugos institucija naudoja veido atpažinimo technologiją savo užduotims, patenkančioms į Teisėsaugos direktyvos taikymo sritį (nusikalstamų veikų prevencija, tyrimas ar baudžiamasis persekiojimas už jas ir kt. pagal Teisėsaugos direktyvos 3 straipsnį), ji gali būti laikoma su veido atpažinimo technologijos naudojimu susijusių duomenų valdytoja. Tačiau teisėsaugos institucijos yra sudarytos iš kelių skyrių ir (arba) padalinių, kurie gali dalyvauti šiame duomenų tvarkymo procese, apibrėždami veido atpažinimo technologijos taikymo procesą arba ją praktiškai taikydami. Dėl šios technologijos ypatumų gali prireikti įvairių padalinių, kurie padėtų atlikti jos veiksmingumo matavimus arba toliau ją mokytų.

Su veido atpažinimo technologija susijusiame projekte teisėsaugos institucijoje yra keletas suinteresuotųjų subjektų[70], kuriuos gali reikėti įtraukti:

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

[70] Toliau nurodytos funkcijos atspindi įvairius suinteresuotuosius subjektus ir jų pareigas įgyvendinant veido atpažinimo technologijos projektą. Nors šiame priede vartojamos formuluotės funkcijoms apibūdinti nėra

- vyresnioji vadovybė – patvirtinti projektą, įvertinus riziką ir galimą naudą;
- teisėsaugos institucijos DAP ir (arba) teisės skyrius – padėti įvertinti tam tikro veido atpažinimo technologijos projekto įgyvendinimo teisėtumą; padėti atlikti PDAV; užtikrinti pagarbą duomenų subjektų teisėms ir naudojimąsi jomis;
- proceso savininkas – veikia kaip konkretus kompetentingos teisėsaugos institucijos padalinys, atsakingas už projekto rengimą, sprendžia dėl veido atpažinimo technologijos projekto detalių, įskaitant sistemos veiksmingumo reikalavimus, sprendžia dėl tinkamo sąžiningumo rodiklio, nustato patikimumo įvertinimą[71]; nustato priimtinas šališkumo ribas; nustato galimus pavojus, kuriuos veido atpažinimo technologijos projektas kelia asmenų teisėms ir laisvėms (taip pat konsultuojantis su DAP ir IT DI ir (arba) duomenų mokslo padaliniu (žr. toliau), ir pateikia juos vyresniajai vadovybei. Proceso savininkas, prieš priimdamas sprendimą dėl veido atpažinimo technologijos projekto detalių, taip pat konsultuosis su etaloninės duomenų bazės valdytoju, kad suprastų ne tik etaloninės duomenų bazės naudojimo paskirtį, bet ir jos technines detales. Iš naujo mokant įsigytą veido atpažinimo technologiją proceso savininkas taip pat bus atsakingas už mokymo duomenų rinkinio pasirinkimą. Kadangi proceso savininkas yra skyrius, kuriam pavesta parengti projekto detales ir priimti sprendimus dėl jų, jis yra atsakingas už PDAV atlikimą;
- IT DI ir (arba) duomenų mokslo skyrius – padėti atlikti PDAV; paaiškinti turimus parametrus, pagal kuriuos būtų galima įvertinti sistemos veiksmingumą, sąžiningumą[72] ir galimą šališkumą; įgyvendinti technologiją ir technines apsaugos priemones, siekiant užkirsti kelią neteisėtai prieigai prie surinktų duomenų, kibernetiniams išpuoliams ir kt. Iš naujo mokant įsigytą veido atpažinimo technologiją IT DI arba duomenų mokslo padalinys išmokys sistemą, remdamasis proceso savininko pateiktu mokymo duomenų rinkiniu. Šis padalinys taip pat bus atsakingas už priemonių, kuriomis siekiama sumažinti proceso savininkų bendrai nustatytą riziką (pvz., su dirbtiniu intelektu susijusią riziką, kaip antai modeliuojamus duomenų rinkimo išpuolius), nustatymą;
- galutiniai naudotojai (pvz., policijos pareigūnai, dirbantys vietose arba kriminalistikos laboratorijose) – atlikti palyginimą su duomenų baze; kritiškai peržiūrėti rezultatus atsižvelgiant į ankstesnius įrodymus ir pateikti proceso savininkui grįžtamąją informaciją dėl klaidingai teigiamų rezultatų ir galimos diskriminacijos požymių;
- etaloninės duomenų bazės valdytojas – specialus kompetentingos teisėsaugos institucijos skyrius, atsakingas už etaloninės duomenų bazės, t. y. duomenų bazės, su kuria bus lyginami atvaizdai, pildymą ir tvarkymą, įskaitant veido atvaizdų ištrynimą pasibaigus nustatytam saugojimo laikotarpiui. Tokia duomenų bazė gali būti sukurta specialiai numatomam veido atpažinimo technologijos projektui arba gali egzistuoti iš anksto suderinamumo tikslais. Etaloninės duomenų bazės valdytojui pavesta nustatyti, kada ir kokiomis aplinkybėmis galima saugoti veido atvaizdus, taip pat nustatyti jų duomenų saugojimo reikalavimus (atsižvelgiant į laiką arba kitus kriterijus).

Kadangi dauguma veido atpažinimo technologijos diegimo ir naudojimo atvejų kyla iš esmės didelis pavojus duomenų subjektų teisėms ir laisvėms, duomenų apsaugos priežiūros institucija taip pat turėtų dalyvauti išankstinėse konsultacijose, kurių reikalaujama pagal Teisėsaugos direktyvos 28 straipsnį.

konkrečios, kiekviena teisėsaugos institucija turi apibrėžti ir priskirti panašias funkcijas pagal savo organizacinę struktūrą. Gali būti, kad padalinys atlieka daugiau nei vieną funkciją, pavyzdžiui, proceso savininko ir etaloninės duomenų bazės valdytojo arba proceso savininko ir IT DI ir (arba) duomenų mokslo padalinio (jei proceso savininko skyrius turi visas reikiamas technines žinias).

[71] Patikimumo įvertinimas – tai prognozės (atitikties) patikimumo lygis, išreikštas kaip tikimybė. Pvz., palyginus du šablonus, yra 90 % tikimybė, kad jie priklauso tam pačiam asmeniui. Patikimumo įvertinimas skiriasi nuo veido atpažinimo technologijos veiksmingumo, tačiau jis turi įtakos veiksmingumui. Kuo didesnė patikimumo riba, tuo mažiau klaidingų teigiamų rezultatų ir tuo daugiau klaidingų neigiamų rezultatų pateikiama veido atpažinimo technologijos rezultatuose.

[72] Sąžiningumas gali būti apibrėžiamas kaip nesąžiningos, neteisėtos diskriminacijos, pavyzdžiui, diskriminacijos dėl lyties ar rasės, nebuvimas.

2. VEIDO ATPAŽINIMO TECHNOLOGIJOS SISTEMOS NAUDOJIMO PRADŽIA / PRIEŠ JĄ ĮSIGYJANT

Teisėsaugos institucijos proceso savininkas pirmiausia turėtų aiškiai suprasti procesą (-us), kuriuo (-iais) siekiama naudoti veido atpažinimo technologiją (naudojimo atvejį (-us)), ir užtikrinti, kad būtų teisinis pagrindas pagrįsti numatomo naudojimo atvejį. Remdamiesi tuo, jie turi:

- oficialiai apibūdinti naudojimo atvejį. Turi būti aprašyta spręstina problema ir tai, kaip veido atpažinimo technologija bus rastas sprendimas, taip pat proceso (užduoties), kuriame ji bus taikoma, apžvalga. Šiuo atžvilgiu teisėsaugos institucijos turėtų įrašyti bent šiuos duomenis[73]:
  - proceso metu registruojamų asmens duomenų kategorijas;
  - tikslus ir konkrečius tikslus, kuriais bus naudojama veido atpažinimo technologija, įskaitant galimas pasekmes duomenų subjektui nustačius atitiktį;
  - kada ir kaip bus renkami veido atvaizdai (įskaitant informaciją apie tokio rinkimo kontekstą, pvz., prie oro uosto vartų, vaizdo įrašai iš apsaugos kamerų prie parduotuvės, kurioje buvo padarytas nusikaltimas, ir kt., ir duomenų subjektų, kurių biometriniai duomenys bus tvarkomi, kategorijas);
  - duomenų bazę, su kuria bus lyginami vaizdai (etaloninė duomenų bazė), taip pat informaciją apie tai, kaip ji buvo sukurta, jos dydį ir joje esančių biometrinių duomenų kokybę;
  - teisėsaugos institucijos subjektus, kuriems bus suteikti įgaliojimai naudoti veido atpažinimo technologijos sistemą ir veikti pagal ją teisėsaugos srityje (jų profilius ir prieigos teises turi apibrėžti proceso savininkas);
  - numatytą įvestų duomenų saugojimo laikotarpį arba momentą, kuris nulems šio laikotarpio pabaigą (pvz., baudžiamojo proceso, dėl kurio jie pirma buvo surinkti, užbaigimas arba nutraukimas pagal nacionalinę proceso teisę), taip pat bet kokius vėlesnius veiksmus (šių duomenų ištrynimą, nuasmeninimą ir naudojimą statistikos ar mokslinių tyrimų tikslais ir kt.);
  - registravimo įgyvendinimą ir galimybę susipažinti su saugomais įrašais;
  - veiksmingumo parametrus (pvz., tikslumą, atšaukimą, F1 įvertinimą) ir jų mažiausias priimtinumo ribas[74];
  - įvertį, kiek asmenų bus taikoma veido atpažinimo technologija, kuriuo laikotarpiu ir kokiu atveju;
- atlikti būtinumo ir proporcingumo vertinimą[75]. Tai, kad tokia technologija egzistuoja, neturėtų paskatinti jos taikyti. Proceso savininkas pirmiausia turi įvertinti, ar egzistuoja tinkamas teisinis pagrindas numatytam duomenų tvarkymui. Šiuo tikslu reikia konsultuotis su DAP ir teisės tarnyba. Įdiegti veido atpažinimo technologiją turėtų paskatinti tai, kad ji yra būtinas ir proporcingas sprendimas konkrečiai apibrėžtai teisėsaugos institucijų problemai spręsti. Tai reikia įvertinti

[73] I priede pateikiamas elementų, padedančių duomenų valdytojui apibūdinti veido atpažinimo technologijos naudojimo atvejį, sąrašas.

[74] Esama įvairių parametrų, pagal kuriuos vertinamas veido atpažinimo technologijos sistemos veiksmingumas. Kiekvienu parametru galima susidaryti skirtingą sistemos rezultatų vaizdą, o jos sėkmė tinkamai parodant, ar veido atpažinimo technologija veikia gerai ar ne, priklauso nuo veido atpažinimo technologijos naudojimo atvejo. Jei pagrindinis dėmesys skiriamas tam, kad būtų pasiektas aukštas procentas teisingų veido atitikčių, galima naudoti tokius parametrus, kaip tikslumas ir atkūrimas. Tačiau šiais parametrais neįvertinama, kaip gerai veido atpažinimo technologija susidoroja su neigiamais pavyzdžiais (kiek jų sistema sutapatino neteisingai). Proceso savininkas, padedamas IT DI ir duomenų mokslo padalinio, turėtų galėti nustatyti veiksmingumo reikalavimus ir tada išreikšti juos tinkamiausiais parametrais pagal veido atpažinimo technologijos naudojimo atvejį.

[75] Siekiant užtikrinti būtinumą, gali būti svarstomi tolesni veiksmai, susiję su sistemos pritaikymu ir naudojimu, todėl atliekant būtinumo ir proporcingumo vertinimą naudojimo atvejo aprašymas taip pat gali būti šiek tiek pakeistas.

atsižvelgiant į nusikaltimų tikslą, sunkumą ir (arba) asmenų, kurie su nusikaltimu nėra susiję, bet kuriems veido atpažinimo technologijos sistema daro poveikį, skaičių. Siekiant įvertinti teisėtumą, reikėtų atsižvelgti bent į šiuos dokumentus: Teisėsaugos direktyvą[76], BDAR[77] [78], bet kokią esamą teisinę sistemą dėl dirbtinio intelekto[79] ir visas susijusias duomenų apsaugos priežiūros institucijų pateiktas gaires (pavyzdžiui, EDAV gaires 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus[80]). Šie ES teisės aktai visada turėtų būti suderinti su taikytinais nacionaliniais reikalavimais, ypač baudžiamojo proceso teisės srityje. Atliekant proporcingumo vertinimą turėtų būti nustatytos duomenų subjektų pagrindinės teisės, kurioms gali būti padarytas poveikis (neapsiribojant privatumu ir duomenų apsauga). Jame taip pat turėtų būti aprašyti ir apsvarstyti visi veido atpažinimo technologijos naudojimo atveju nustatyti apribojimai (arba apribojimų nebuvimas). Pavyzdžiui, ar sistema veiks nepertraukiamai arba laikinai ir tik tam tikroje geografinėje vietoje;

- atlikti poveikio duomenų apsaugai vertinimą (PDAV)[81]. PDAV reikėtų atlikti, nes veido atpažinimo technologijos diegimas teisėsaugos srityje gali sukelti didelį pavojų asmenų teisėms ir laisvėms[82]. PDAV visų pirma turėtų būti pateiktas bendras numatytų duomenų tvarkymo operacijų aprašymas[83], pavojaus duomenų subjektų teisėms ir laisvėms įvertinimas[84], numatytos priemonės šiam pavojui pašalinti, apsaugos priemonės, saugumo priemonės ir mechanizmai, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi reikalavimų. PDAV yra tęstinis procesas, todėl reikėtų įtraukti visus naujus duomenų tvarkymo elementus ir atnaujinti rizikos vertinimą kiekviename projekto etape;
- gauti vyresniosios vadovybės pritarimą, paaiškindami pavojus duomenų subjektų teisėms ir laisvėms (pagal naudojimo atvejį ir technologiją) ir atitinkamus veiksmų su rizika planus;

[76] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais.

[77] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.

[78] Tais atvejais, kai vykdant mokslinį projektą, kuriuo siekiama ištirti veido atpažinimo technologijos naudojimą, reikėtų tvarkyti asmens duomenis, tačiau tokiam tvarkymui nebūtų taikoma Teisėsaugos direktyvos 4 straipsnio 3 dalis, paprastai būtų taikomas BDAR (Teisėsaugos direktyvos 9 straipsnio 2 dalis). Bandomųjų projektų, po kurių būtų vykdomos teisėsaugos operacijos, atveju Teisėsaugos direktyva vis tiek būtų taikoma.

[79] Pavyzdžiui, pateiktas pasiūlymas dėl EUROPOS PARLAMENTO IR TARYBOS REGLAMENTO, KURIUO NUSTATOMOS SUDERINTOS TAISYKLĖS DĖL DIRBTINIO INTELEKTO (DIRBTINIO INTELEKTO AKTAS) IR IŠ DALIES PAKEIČIAMI TAM TIKRI SĄJUNGOS TEISĖS AKTAI, tačiau jis dar nėra priimtas kaip reglamentas.

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

[81] Daugiau rekomendacijų dėl PDAV galima rasti Poveikio duomenų apsaugai vertinimo (PDAV) gairėse, kuriomis Reglamento (ES) 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, WP248, 1-oji peržiūrėta versija, paskelbtose adresu https://ec.europa.eu/newsroom/article29/items/611236, ir EDAPP atskaitomybės vykdant veiksmus vietoje priemonių rinkinyje, II dalis, paskelbtame adresu https://edps.europa.eu/node/4582_en.

[82] Veido atpažinimo technologija, priklausomai nuo naudojimo atvejo, gali atitikti toliau nurodytus kriterijus, dėl kurių pradedamas didelį pavojų keliantis duomenų tvarkymas (DPAV gairės, WP248, 1-oji peržiūrėta versija): sisteminga stebėsena, didelio masto duomenų tvarkymas, duomenų rinkinių siejimas ir derinimas, naujoviškas naudojimas arba naujų technologinių ar organizacinių sprendimo būdų taikymas.

[83] Be rizikos vertinimo, duomenų tvarkymo aprašymas, taip pat būtinumo ir proporcingumo įvertinimas, kaip jau aprašyta pirmiau nurodytuose etapuose, yra dar viena PDAV dalis. Prireikus PDAV bus pateiktas išsamesnis asmens duomenų srautų aprašymas.

[84] Duomenų subjektams kylančio pavojaus analizė turėtų apimti pavojus, susijusius su lygintinų veido atvaizdų vieta (vietoje / nuotoliniu būdu), pavojų, susijusį su duomenų tvarkytojais ir (arba) pagalbiniais duomenų tvarkytojais, taip pat pavojus, būdingus mašininiam mokymuisi, kai jis taikomas (pvz., duomenų užkrėtimą, priešiškus pavyzdžius).

3. VIEŠŲJŲ PIRKIMŲ METU IR PRIEŠ PRADEDANT TAIKYTI VEIDO ATPAŽINIMO TECHNOLOGIJĄ

- nuspręsti, pagal kokius kriterijus pasirinkti veido atpažinimo technologiją (algoritmą). Proceso savininkas, padedamas IT DI ir (arba) duomenų mokslo padalinio, turėtų nuspręsti, pagal kokius kriterijus pasirinkti algoritmą. Praktiškai tai apimtų sąžiningumo ir veiksmingumo parametrus, dėl kurių nuspręsta naudojimo atvejo aprašyme. Tokie kriterijai taip pat turėtų apimti informaciją, susijusią su duomenimis, su kuriais algoritmas buvo apmokytas. Siekiant sumažinti šališkumą, mokymo, bandymo ir patvirtinimo rinkiniuose turi būti pakankamai visų duomenų subjektų, kuriems bus taikoma veido atpažinimo technologija, charakteristikų pavyzdžių (pavyzdžiui, amžiaus, lyties ir rasės). Veido atpažinimo technologijos teikėjas turėtų pateikti informaciją ir parametrus apie veido atpažinimo technologijos mokymo, bandymo ir patvirtinimo duomenų rinkinius ir aprašyti priemones, kurių imtasi galimai neteisėtai diskriminacijai ir šališkumui įvertinti ir sumažinti. Kai įmanoma, proceso savininkas turi patikrinti, ar yra teisinis pagrindas paslaugų teikėjui naudoti šį duomenų rinkinį algoritmų mokymo tikslais (remdamasis informacija, kurią pateiks teikėjas). Be to, proceso savininkas turėtų užtikrinti, kad veido atpažinimo technologijos teikėjas taikytų su biometriniais duomenimis susijusius saugumo standartus, pvz., ISO/IEC 24745, kuriuose pateikiamos gairės dėl biometrinės informacijos apsaugos pagal įvairius konfidencialumo, vientisumo ir atnaujinimo / atšaukiamumo reikalavimus saugojimo ir perdavimo metu, taip pat saugaus ir privatumą atitinkančio biometrinės informacijos valdymo ir tvarkymo reikalavimus ir gaires;

- iš naujo mokyti algoritmą (jei reikia). Proceso savininkas turėtų užtikrinti, kad veido atpažinimo technologijos sistemos derinimas siekiant didesnio tikslumo prieš pradedant ją naudoti taip pat būtų perkamų paslaugų dalis. Jeigu būtinas papildomas įsigytos veido atpažinimo technologijos sistemos mokymas siekiant atitikti tikslumo parametrus, proceso savininkas, padedamas IT DI ir (arba) duomenų mokslo padalinio, turi ne tik priimti sprendimą iš naujo mokyti, bet ir nuspręsti dėl tinkamo, reprezentatyviojo duomenų rinkinio, kurį būtų galima naudoti, ir patikrinti šio duomenų naudojimo teisėtumą;
- nustatyti tinkamas apsaugos priemones rizikai, susijusiai su saugumu, šališkumu ir mažu veiksmingumu, valdyti. Tai apima veido atpažinimo technologijos stebėsenos proceso nustatymą, kai ji bus naudojama (registravimas ir grįžtamoji informacija, siekiant užtikrinti rezultatų tikslumą ir teisingumą). Be to, reikia pasirūpinti, kad būtų nustatyti, įvertinti ir sumažinti pavojai, būdingi tam tikroms mašininio mokymosi ir veido atpažinimo technologijos sistemoms (pvz., duomenų užkrėtimas, priešiški pavyzdžiai, modelio inversija, „baltosios dėžės“ testavimo išvada). Proceso savininkas taip pat turėtų nustatyti tinkamas apsaugos priemones, kuriomis būtų užtikrinta, kad į mokymo iš naujo duomenų rinkinį įtrauktų biometrinių duomenų saugojimo reikalavimų būtų laikomasi;
- dokumentuoti veido atpažinimo technologijos sistemą. Tai turėtų apimti bendrą veido atpažinimo technologijos sistemos aprašymą, išsamų veido atpažinimo technologijos elementų ir jos sukūrimo proceso aprašymą, išsamią informaciją apie veido atpažinimo technologijos stebėseną, veikimą ir kontrolę, taip pat išsamų jos rizikos ir rizikos mažinimo priemonių aprašymą. Bus dokumentuojami pagrindiniai ankstesnių etapų veido atpažinimo technologijos sistemos aprašymo elementai (žr. pirmiau), tačiau jie bus papildyti informacija, susijusia su stebėsenos veiksmingumu ir sistemos pakeitimų taikymu, įskaitant bet kokius versijų atnaujinimus ir (arba) mokymą iš naujo;
- parengti naudotojo vadovus, kuriuose būtų paaiškinta technologija ir naudojimo atvejai. Juose turi būti aiškiai paaiškinti visi scenarijai ir išankstinės sąlygos, pagal kurias bus taikoma veido atpažinimo technologija;

- mokyti galutinius naudotojus, kaip naudotis šia technologija. Tokiuose mokymuose reikia paaiškinti technologijos galimybes ir apribojimus, kad naudotojai suprastų, kokiomis aplinkybėmis ją būtina taikyti ir kokiais atvejais ji gali būti netiksli. Tokie mokymai taip pat padės sumažinti riziką, susijusią su algoritmo rezultatų netikrinimu ir (arba) nekritiniu vertinimu;
- konsultuotis su duomenų apsaugos priežiūros institucija pagal Teisėsaugos direktyvos 28 straipsnio 1 dalies b punktą; pateikti informaciją pagal Teisėsaugos direktyvos 13 straipsnį, kad duomenų subjektai būtų informuoti apie duomenų tvarkymą ir savo teises. Šie pranešimai duomenų subjektams turi būti parengti tinkama kalba, kad jie galėtų suprasti duomenų tvarkymą, juose reikėtų paaiškinti pagrindinius technologijos elementus, įskaitant tikslumo rodiklius, mokymo duomenų rinkinius ir priemones, kurių imtasi siekiant išvengti diskriminacijos ir nepakankamo algoritmo tikslumo;

4. REKOMENDACIJOS PO VEIDO ATPAŽINIMO TECHNOLOGIJOS ĮDIEGIMO

- užtikrinti žmogaus įsikišimą ir rezultatų priežiūrą. Niekada nesiimti jokių su asmeniu susijusių priemonių remiantis vien tik veido atpažinimo technologijos rezultatais (tai reikštų, kad pažeidžiamas Teisėsaugos direktyvos 11 straipsnis – automatizuotas individualių sprendimų priėmimas, turintis teisinį ar panašų poveikį duomenų subjektui). Užtikrinti, kad teisėsaugos institucijos pareigūnas peržiūrėtų veido atpažinimo technologijos taikymo rezultatus. Taip pat užtikrinti, kad teisėsaugos institucijų naudotojai išvengtų automatizavimo šališkumo, tirdami prieštaringą informaciją ir kritiškai vertindami technologijos taikymo rezultatus. Todėl svarbu nuolat mokyti galutinius naudotojus ir didinti jų informuotumą, tačiau vyresnioji vadovybė turėtų užtikrinti, kad būtų pakankamai žmogiškųjų išteklių veiksmingai priežiūrai vykdyti. Tai reiškia, kad kiekvienam pareigūnui turi būti suteikta pakankamai laiko kritiškai įvertinti technologijos rezultatus. Registruoti, išmatuoti ir įvertinti, kiek žmogaus vykdoma priežiūra keičia pirminį veido atpažinimo technologijos sprendimą;
- stebėti ir spręsti veido atpažinimo technologijos modelio dreifo (veiksmingumo blogėjimo) klausimus, kai modelis kuriamas;
- nustatyti procesą, pagal kurį reguliariai ir kaskart, kai pasikeičia technologija ar naudojimo atvejis, iš naujo įvertinami pavojai ir saugumo priemonės;
- dokumentuoti visus sistemos pakeitimus per visą jos gyvavimo ciklą (pvz., atnaujinimus, mokymą iš naujo);
- nustatyti procesą ir susijusias technines galimybes, kad būtų galima nagrinėti duomenų subjektų prašymus leisti susipažinti su duomenimis. Techninės galimybės gauti duomenis, jei juos reikėtų pateikti duomenų subjektams, turi būti sukurtos dar prieš gaunant bet kokį prašymą;
- užtikrinti, kad būtų įdiegtos duomenų saugumo pažeidimų procedūros. Įvykus asmens duomenų saugumo pažeidimui, susijusiam su biometriniais duomenimis, tikėtina, kad kils didelė rizika. Šiuo atveju visi susiję naudotojai turėtų žinoti apie atitinkamas procedūras, kurių reikia laikytis, DAP ir duomenų subjektai turėtų būti nedelsiant informuojami.

III PRIEDAS. PRAKTINIAI PAVYZDŽIAI

Yra daug įvairių praktinių veido atpažinimo naudojimo situacijų ir tikslų, pavyzdžiui, kontroliuojamoje aplinkoje, kaip antai sienos perėjimo punktuose, kryžminis patikrinimas su duomenimis iš policijos duomenų bazių arba asmens duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai, tiesioginės vaizdo transliacijos (veido atpažinimas tikruoju laiku) ir kt. Todėl asmens duomenų ir kitų pagrindinių teisių ir laisvių apsaugai kylanti rizika skirtingais naudojimo atvejais labai skiriasi. Siekiant palengvinti būtinumo ir proporcingumo vertinimą, kuris turėtų būti atliekamas prieš priimant sprendimą dėl galimo veido atpažinimo technologijos taikymo, šiose gairėse pateikiamas nebaigtinis galimų veido atpažinimo technologijos taikymo būdų teisėsaugos srityje sąrašas.

Pateikti ir įvertinti scenarijai grindžiami **hipotetinėmis** situacijomis ir jais siekiama parodyti tam tikrus konkrečius veido atpažinimo technologijos naudojimo būdus ir suteikti pagalbą kiekvienu konkrečiu atveju, taip pat nustatyti bendrą sistemą. Jie nėra išsamūs ir nedaro poveikio jokiems nacionalinės priežiūros institucijos vykdomiems ar būsimiems procesams, susijusiems su veido atpažinimo technologijų kūrimu, eksperimentavimu ar įgyvendinimu. Šie scenarijai turėtų tik pavaizduoti šiame dokumente jau pateiktas gaires politikos formuotojams, teisės aktų leidėjams ir teisėsaugos institucijoms rengiant ir numatant veido atpažinimo technologijų įgyvendinimą, siekiant užtikrinti visapusišką atitiktį ES *acquis* asmens duomenų apsaugos srityje. Šiomis aplinkybėmis reikėtų nepamiršti, kad net ir panašiais atvejais, kai naudojama veido atpažinimo technologija, tam tikrų elementų buvimas arba nebuvimas gali lemti kitokį būtinumo ir proporcingumo vertinimo rezultatą.

1 1 SCENARIJUS

1.1. Aprašymas

Automatizuota sienų kontrolės sistema, leidžianti automatiškai pereiti sieną patvirtinant ES piliečių ir kitų keliautojų, kertančių sieną sienos perėjimo punkte, elektroniniame kelionės dokumente saugomų biometrinių duomenų autentiškumą ir nustatant, kad keleivis yra teisėtas dokumento turėtojas.

Tokia patikra ir (arba) autentiškumo patvirtinimas apima tik veido atpažinimą lyginant „1 su 1“ ir atliekamas kontroliuojamoje aplinkoje (pvz., prie oro uosto e. vartų). Sieną kertančio keleivio biometriniai duomenys užfiksuojami, kai jis aiškiai paprašomas pažvelgti į e. vartų kamerą, ir palyginami su pateikto dokumento (paso, asmens tapatybės kortelės ir kt.), kuris išduodamas laikantis konkrečių techninių reikalavimų, biometriniais duomenimis.

Tuo pat metu, nors tokiais atvejais duomenų tvarkymas iš esmės nepatenka į Teisėsaugos direktyvos taikymo sritį, patikrinimo rezultatai taip pat gali būti naudojami (raidiniams skaitmeniniams) asmens duomenims palyginti teisėsaugos duomenų bazėse vykdant sienų kontrolę ir todėl gali būti susiję su veiksmais, kurie turi didelį teisinį poveikį duomenų subjektui, pvz., dėl perspėjimo SIS jis gali būti areštuotas. Tam tikromis aplinkybėmis biometriniai duomenys taip pat gali būti naudojami ieškant atitikčių teisėsaugos institucijų duomenų bazėse (tokiu atveju šiame etape būtų atliekamas tapatybės patvirtinimas „1 su daugeliu“).

Biometrinių atvaizdų tvarkymo rezultatai turi tiesioginį poveikį duomenų subjektui – sieną galima kirsti tik jeigu duomenų patikrinimas buvo sėkmingas. Nepavykus nustatyti asmens tapatybės, sienos apsaugos pareigūnai turi atlikti antrą patikrinimą, kad įsitikintų, jog duomenų subjektas skiriasi nuo to, kuris nurodytas tapatybės dokumente.

Jeigu gaunamas SIS ar nacionalinis perspėjimas, sienos apsaugos pareigūnai turi atlikti antrą patikrinimą ir būtinus papildomus patikrinimus, o tada imtis visų būtinų veiksmų, pvz., areštuoti asmenį, informuoti susijusias institucijas.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ visi sienas kertantys asmenys
- Atvaizdo šaltinis: ☒ kita (asmens tapatybės dokumentas)
- Ryšys su nusikaltimu: ☒ Nebūtinas
- Informacijos užfiksavimo būdas: ☒ kabinoje arba kontroliuojamoje aplinkoje
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms: Taip, būtent: ☒ teisei į laisvą judėjimą ☒ teisei į prieglobstį

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☒ specialios paskirties duomenų bazės, susijusios su sienų kontrole

Algoritmas:

- Patikrinimo tipas: ☒ patikrinimas „1 su 1“ (tapatybės patvirtinimas)

Rezultatai:

- Poveikis ☒ Tiesioginis (duomenų subjektui leidžiama arba neleidžiama atvykti)
- Automatizuotas sprendimas: ☒ Taip

1.2. Taikytina teisinė sistema

Nuo 2004 m. pagal Tarybos reglamentą (EB) Nr. 2252/2004[85] valstybių narių išduodamuose pasuose ir kituose kelionės dokumentuose turi būti biometrinis veido atvaizdas, saugomas dokumente įmontuotame elektroniniame luste.

Šengeno sienų kodekse[86] nustatyti asmenų tikrinimo prie išorės sienų reikalavimai. ES piliečių ir kitų asmenų, turinčių laisvo judėjimo teisę pagal Sąjungos teisę, būtiniausi patikrinimai turėtų apimti jų kelionės dokumentų patikrinimą, prireikus naudojant techninius prietaisus. Šengeno sienų kodeksas vėliau buvo iš dalies pakeistas Reglamentu (ES) 2017/2225[87], kuriame, *inter alia*, nustatytos sąvokų „e. vartai“, „automatizuotos sienų kontrolės sistema“ ir „savitarnos sistema“ apibrėžtys, taip pat galimybė tvarkyti biometrinius duomenis atliekant patikrinimus kertant sieną.

Todėl galima daryti prielaidą, kad yra aiškus ir nuspėjamas teisinis pagrindas, kuriuo remiantis leidžiama atlikti tokio pobūdžio asmens duomenų tvarkymą. Be to, teisinė sistema priimta Sąjungos lygmeniu ir tiesiogiai taikoma valstybėms narėms.

1.3. Būtinumas ir proporcingumas – tikslas / nusikaltimo sunkumas

ES piliečių tapatybės tikrinimas automatizuotos sienų kontrolės sistemoje, naudojant jų biometrinį atvaizdą, yra ES sienų kontrolės prie išorės sienų dalis. Todėl jis yra tiesiogiai susijęs su sienų saugumu ir atitinka Sąjungos pripažįstamą bendrojo intereso tikslą. Be to, automatizuotos sienų kontrolės vartai padeda paspartinti keleivių srauto patikrinimą ir sumažinti žmogaus klaidų riziką. Be to, suvaržymo apimtis, mastas ir intensyvumas šiame scenarijuje yra daug mažesni, palyginti su kitų formų veido atpažinimu. Vis dėlto biometrinių duomenų tvarkymas kelia duomenų subjektams papildomą riziką,

[85] 2004 m. gruodžio 13 d. TARYBOS REGLAMENTAS (EB) Nr. 2252/2004 dėl valstybių narių išduodamų pasų ir kelionės dokumentų apsauginių savybių ir biometrikos standartų.

[86] 2016 m. kovo 9 d. EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS (ES) 2016/399 dėl taisyklių, reglamentuojančių asmenų judėjimą per sienas, Sąjungos kodekso (Šengeno sienų kodeksas).

[87] 2017 m. lapkričio 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2225, kuriuo iš dalies keičiamos Reglamento (ES) 2016/399 nuostatos, susijusios su atvykimo ir išvykimo sistemos naudojimu.

kurią turi tinkamai įvertinti ir sumažinti veido atpažinimo technologiją įdiegusi ir naudojanti kompetentinga institucija.

1.4. Išvada

ES piliečių tapatybės tikrinimas vykdant automatizuotą sienų kontrolę yra būtina ir proporcinga priemonė, jei taikomos tinkamos apsaugos priemonės, visų pirma tikslo ribojimo, duomenų kokybės, skaidrumo ir aukšto lygio saugumo principai.

2 2 SCENARIJUS

2.1. Aprašymas

Teisėsaugos institucijos sukuria vaikų pagrobimo aukų tapatybės nustatymo sistemą. Įgaliotasis policijos pareigūnas griežtomis sąlygomis gali palyginti vaiko, kuris, kaip įtariama, yra pagrobtas, biometrinius duomenis su vaikų pagrobimo aukų duomenų baze tik tam, kad nustatytų nepilnamečių, kurie gali atitikti dingusio vaiko, dėl kurio pradėtas tyrimas ir paskelbtas perspėjimas, aprašymą, tapatybę.

Duomenų tvarkymas būtų susijęs su asmens, kuris gali atitikti dingusio vaiko aprašymą, veido arba atvaizdo palyginimu su duomenų bazėje saugomais vaizdais. Toks duomenų tvarkymas būtų vykdomas konkrečiais atvejais, o ne sistemingai.

Duomenų bazė, su kuria bus lyginama, pildoma dingusių vaikų, dėl kurių buvo pranešta apie įtariamą vaikų pagrobimą, grėsmę vaiko gyvybei ar fizinei neliečiamybei, dėl kurių teisminė institucija pradėjo baudžiamąjį tyrimą ir dėl kurių buvo paskelbtas perspėjimas dėl vaikų pagrobimo, nuotraukomis. Duomenys renkami laikantis kompetentingos teisėsaugos institucijos, t. y. policijos pareigūnų, įgaliotų vykdyti teismines policijos užduotis, nustatytų procedūrų. Registruojamų asmens duomenų kategorijos:

- tapatybė, slapyvardis, *alias*, giminystės ryšys, pilietybė, adresai, el. pašto adresai, telefono numeriai;
- gimimo data ir vieta;
- informacija apie tėvystę;
- nuotrauka su techninėmis savybėmis, kurios leidžia naudoti veido atpažinimo prietaisą, ir kitos nuotraukos.

Įgaliotasis pareigūnas taip pat turi peržiūrėti ir patikrinti palyginimo rezultatus, kad būtų galima patvirtinti ankstesnius įrodymus palyginimo rezultatais ir atmesti bet kokius galimus klaidingus teigiamus rezultatus.

Vaikų nuotraukos ir asmens duomenys gali būti saugomi tik tol, kol galioja perspėjimas, ir turi būti ištrinami iš karto po to, kai baudžiamasis procesas pagal nacionalines procedūras, dėl kurio jie buvo įtraukti į duomenų bazę, užbaigiamas arba nutraukiamas.

Nors duomenų bazėje gali būti numatytas palyginti ilgas biometrinių duomenų saugojimo laikotarpis, apibrėžtas pagal nacionalinę teisę, naudojimasis duomenų subjektų teisėmis, visų pirma teise reikalauti ištaisyti ir ištrinti duomenis, suteikia papildomą garantiją, kad atitinkamų duomenų subjektų teisės į asmens duomenų apsaugą suvaržymas būtų apribotas.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ Vaikai
- Atvaizdo šaltinis ☒ kita: iš anksto nenustatyta, įtariama vaikų grobimo auka
- Ryšys su nusikaltimu ☒ Netiesioginis laikinis ☒ Netiesioginis geografinis
- Informacijos užfiksavimo būdas: ☒ kabinoje arba kontroliuojamoje aplinkoje
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms ☒ Taip, būtent: ☒ įvairioms

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas ☒ speciali duomenų bazė

Algoritmas:

- Patikrinimo tipas: ☒ tapatybės nustatymas „1 su daugeliu“

Rezultatai:

- Poveikis ☒ Tiesioginis
- Automatizuotas sprendimas: ☒ NE, privaloma įgaliotojo pareigūno peržiūra

Teisinė analizė:

- Taikytina teisinė sistema: ☒ Speciali nacionalinės teisės aktai dėl tokio duomenų tvarkymo (veido atpažinimas)

2.2. Taikytina teisinė sistema

Nacionalinėje teisėje numatyta speciali teisinė sistema, kuria sukuriama duomenų bazė, nustatomi duomenų tvarkymo tikslai, taip pat duomenų bazės pildymo, prieigos prie jos ir naudojimo kriterijai. Jo įgyvendinimui būtinose teisėkūros priemonėse taip pat numatytas saugojimo laikotarpio nustatymas, taip pat nuoroda į taikytinus vientisumo ir konfidencialumo principus. Teisėkūros priemonėse taip pat numatytos informacijos teikimo duomenų subjektui ir šiuo atveju asmeniui (-ims), kuriems tenka tėvų pareigos, sąlygos, taip pat duomenų subjektų naudojimasis teisėmis ir, jei taikytina, galimas apribojimas. Rengiant pasiūlymą dėl atitinkamos teisėkūros priemonės reikėjo konsultuotis su nacionaline priežiūros institucija.

2.3. Būtinumas ir proporcingumas – tikslas / nusikaltimo sunkumas / nesusijusių, bet su duomenų tvarkymo paveiktų asmenų skaičius

Duomenų tvarkymo sąlygos ir apsaugos priemonės

Palyginimą naudojant veido atpažinimo technologiją įgaliotas pareigūnas gali atlikti tik kraštutiniu atveju, jei nėra kitų mažesnio poveikio kišimosi priemonių ir jei tai yra būtina, pavyzdžiui, kilus abejonių dėl keliaujančio nepilnamečio asmens tapatybės dokumento autentiškumo ir (arba) peržiūrėjus ankstesnius įrodymus ir surinktą medžiagą, iš kurios matyti, kad vaikas gali atitikti dingusio vaiko, dėl kurio atliekamas baudžiamasis tyrimas, aprašymą.

Taip pat numatyta papildoma apsaugos priemonė, pagal kurią įgaliotasis pareigūnas privalo peržiūrėti ir patikrinti palyginimą naudojant veido atpažinimo technologiją, siekiant patvirtinti ankstesnius įrodymus palyginimo rezultatais ir atmesti bet kokius galimus klaidingus teigiamus rezultatus.

Siekiamas tikslas

Duomenų bazės sukūrimas padeda siekti svarbių bendrojo viešojo intereso tikslų, visų pirma užtikrinti nusikalstamų veikų prevenciją, tyrimą, nustatymą ar patraukimą baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymą ir kitų asmenų teisių ir laisvių apsaugą. Atrodo, kad duomenų bazės sukūrimas ir numatomas duomenų tvarkymas padeda nustatyti vaikų grobimo aukų tapatybę,

todėl tai galima laikyti tinkama priemone teisėtam tokių nusikaltimų tyrimo ir baudžiamojo persekiojimo tikslui remti.

Duomenų bazės paskirtis ir pildymas

Duomenų tvarkymo tikslai yra aiškiai apibrėžti teisės aktuose, o duomenų bazė naudojama tik siekiant nustatyti dingusių vaikų, dėl kurių pranešta apie įtarimą dėl vaiko grobimo ir pradėtas nusikalstamos veikos tyrimas prižiūrint teisminei institucijai ir dėl kurių buvo paskelbtas perspėjimas dėl vaikų grobimo, tapatybę. Teisės aktais nustatytomis duomenų bazės pildymo sąlygomis siekiama griežtai apriboti duomenų subjektų skaičių ir į duomenų bazę įtrauktinus asmens duomenis. Asmuo, kuriam tenka vaiko tėvų pareigos, turi būti informuotas apie atliekamą duomenų tvarkymą ir naudojimosi vaiko teisėmis sąlygas, susijusias su tapatybės nustatymo tikslu numatomu biometrinių duomenų tvarkymu, arba apie duomenų bazėje saugomus vaiko asmens duomenis.

2.4. Išvada

Atsižvelgiant į numatyto duomenų tvarkymo būtinumą ir proporcingumą, taip pat į tai, kad toks asmens duomenų tvarkymas labiausiai atitinka vaiko interesus, ir su sąlyga, kad yra numatytos pakankamos garantijos, ypač užtikrinančios naudojimąsi duomenų subjekto teisėmis, visų pirma atsižvelgiant į tai, kad bus tvarkomi vaikų duomenys, toks duomenų tvarkymas naudojant veido atpažinimo technologiją gali būti laikomas tikriausiai suderinamu su ES teise.

Be to, atsižvelgdama į duomenų tvarkymo rūšį ir naudojamą technologiją, susijusią su dideliu pavojumi atitinkamų duomenų subjektų teisėms ir laisvėms, EDAV mano, kad rengiant pasiūlymą dėl teisėkūros priemonės, kurią turi priimti nacionalinis parlamentas, arba tokia teisėkūros priemone grindžiamos reguliavimo priemonės, susijusios su numatomu duomenų tvarkymu, turi būti iš anksto konsultuojamasi su priežiūros institucija, kad būtų užtikrintas nuoseklumas ir atitiktis taikytinai teisinei sistemai (žr. Teisėsaugos direktyvos 28 straipsnio 2 dalį).

3 3 SCENARIJUS

3.1. Aprašymas

Policijai ėmusis intervencinių priemonių dėl riaušių ir atlikus tyrimus po jų, nemažai asmenų buvo identifikuoti kaip įtariamieji, pavyzdžiui, atliekant ankstesnius tyrimus naudojant AVSS įrašus arba liudytojų parodymus. Šių įtariamųjų nuotraukos lyginamos su asmenų, užfiksuotų AVSS arba mobiliaisiais įrenginiais nusikaltimo vietoje arba aplinkinėse zonose, nuotraukomis.

Siekdama gauti išsamesnių įrodymų apie asmenis, įtariamus dalyvavus riaušėse, kilusiose po demonstracijos, policija sukuria duomenų bazę, kurią sudaro vaizdinė medžiaga, maždaug susijusi su riaušėmis vietos ir laiko atžvilgiu. Į duomenų bazę įtraukiami piliečių policijai pateikti privatūs įrašai, viešojo transporto AVSS medžiaga, policijai priklausanti vaizdo stebėjimo medžiaga ir žiniasklaidoje paskelbta medžiaga be jokių specialių apribojimų ar apsaugos priemonių. Sunkių nusikalstamų veikų rodymas nėra būtina duomenų bazės rinkmenų rinkimo sąlyga. Taigi duomenų bazėje saugomi riaušėse nedalyvavę asmenys, t. y. nemaža procentinė dalis vietos gyventojų, kurie demonstracijos metu vyko pro šalį arba dalyvavo demonstracijoje, bet nedalyvavo riaušėse. Tai tūkstančiai vaizdo įrašų ir vaizdų rinkmenų.

Naudojant veido atpažinimo programinę įrangą, visiems šiose rinkmenose esantiems veidams priskiriami unikalūs veido identifikatoriai. Tada pavienių įtariamųjų veidai automatiškai lyginami su šiais veido identifikatoriais. Duomenų bazė, sudaryta iš visų biometrinių duomenų šablonų, esančių tūkstančiuose vaizdo įrašų ir vaizdų rinkmenų, saugoma tol, kol baigiami visi galimi tyrimai. Teigiamas

atitiktis aptaria atsakingieji pareigūnai, kurie po to priima sprendimą dėl tolesnių veiksmų. Tai gali apimti duomenų bazėje rastos rinkmenos įtraukimą į atitinkamo asmens baudžiamąją bylą ir kitas priemones, pavyzdžiui, to asmens apklausą ar areštą.

Nacionalinėje teisėje numatyta bendro pobūdžio nuostata, pagal kurią biometrinių duomenų tvarkymas siekiant vienareikšmiškai nustatyti fizinio asmens tapatybę yra leistinas, jeigu tai tikrai būtina ir jeigu taikomos tinkamos atitinkamo asmens teisių ir laisvių apsaugos priemonės.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ visi asmenys
- Atvaizdo šaltinis: ☒ viešai prieinamos erdvės ☒ privatus subjektas ☒ kiti asmenys ☒ kita: žiniasklaida
- Ryšys su nusikaltimu: ☒ Nebūtinai tiesioginis geografinis ar laikinis ryšys
- Informacijos užfiksavimo būdas: ☒ nuotolinis
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms: Taip, būtent ☒ susirinkimų laisvei
- Turimi papildomi informacijos apie duomenų subjektą šaltiniai:
  ☒ kita: neatmetama (pvz., naudotasi bankomatais ar eita į parduotuves), nes nuotraukose pateiktų vaizdų motyvų kontroliuoti neįmanoma

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☒ specialios paskirties duomenų bazės, susijusios su nusikaltimo sritimi

Algoritmas:

- Duomenų tvarkymo rūšis: ☒ asmens tapatybės nustatymas „1 su daugeliu“

Rezultatai:

- Poveikis: ☒ Tiesioginis (pvz., duomenų subjektas gali būti suimtas, apklaustas)
- Automatizuotas sprendimas: ☒ NE
- Saugojimo trukmė: kol bus nutraukti visi galimi tyrimai

Teisinė analizė:

- Duomenų subjektui teikiamos išankstinės informacijos duomenų rūšis: ☒ Teisėsaugos institucijos svetainėje apskritai
- Taikytina teisinė sistema : ☒ Teisėsaugos direktyva daugiausia perkelta į nacionalinę teisę ☒ Bendrojo pobūdžio nacionalinės teisės aktai dėl biometrinių duomenų naudojimo teisėsaugos institucijose

3.2. Taikytina teisinė sistema

Kaip paaiškinta pirmiau, teisiniai pagrindai, kuriuose tik pakartojama Teisėsaugos direktyvos 10 straipsnio bendroji nuostata, nėra pakankamai aiškūs, kad asmenims būtų tinkamai nurodytos sąlygos ir aplinkybės, kuriomis teisėsaugos institucijos turi teisę naudoti viešose vietose esančių AVSS įrašus jų veido biometrinių duomenų šablonui sukurti ir palyginti su policijos duomenų bazėmis, kitus turimus AVSS ar privačius įrašus ir kt. Todėl šiame scenarijuje nustatyta teisinė sistema neatitinka minimaliųjų reikalavimų, kad galėtų būti teisiniu pagrindu.

3.3. Būtinumas ir proporcingumas

Šiame pavyzdyje duomenų tvarkymas kelia įvairių susirūpinimą keliančių klausimų pagal būtinumo ir proporcingumo principus dėl kelių priežasčių.

Asmenys nėra įtariami padarę sunkų nusikaltimą. Sunkių nusikalstamų rodymas nėra būtina sąlyga norint naudoti duomenų bazėje, kurioje yra vaizdinė medžiaga, esančias rinkmenas. Be to, tiesioginis laikinis ir geografinis ryšys su nusikaltimu nėra būtina sąlyga norint naudoti duomenų bazėje esančias rinkmenas. Dėl to didelė vietos gyventojų procentinė dalis gali būti saugoma biometrinių duomenų bazėje dar kelerius metus, kol bus užbaigti visi tyrimai.

Nusikaltimo vietos duomenų bazė neapsiriboja tik proporcingumo reikalavimus atitinkančiais vaizdais, todėl surenkama neribotas kiekis vaizdų, kuriuos galima palyginti. Tai prieštarauja duomenų kiekio mažinimo principui. Mažesnis vaizdų kiekis taip pat leistų apsvarstyti nealgoritmines ir mažesnio poveikio suvaržymo priemones, pvz., galimybę pasitelkti ypač gabius atpažintojus[88]

Kadangi pavyzdys paimtas iš protesto aplinkinių zonų, taip pat tikėtina, kad vaizduose atskleidžiamos demonstracijos dalyvių politinės pažiūros, o tai dar vienos specialios kategorijos duomenys, kuriems šis scenarijus gali turėti įtakos. Pagal šį scenarijų neaišku, kaip būtų galima užkirsti kelią šių duomenų rinkimui ir kokiomis apsaugos priemonėmis. Be to, kai duomenų subjektai sužino, kad dėl jų dalyvavimo demonstracijoje jie buvo įtraukti į policijos biometrinių duomenų bazę, tai gali turėti rimtą atgrasomąjį poveikį jų naudojimuisi teise į susirinkimus ateityje.

Duomenų bazėje esančius biometrinių duomenų šablonus taip pat galima palyginti tarpusavyje. Tai leidžia policijai ne tik ieškoti konkretaus asmens visoje jos medžiagoje, bet ir atgaminti kelių dienų trukmės asmens elgesio modelį. Ji taip pat gali surinkti papildomos informacijos apie asmenis, pavyzdžiui, socialinius ryšius ir dalyvavimą politiniame gyvenime.

Suvaržymas dar labiau suintensyvėja dėl to, kad duomenys tvarkomi be duomenų subjektų žinios.

Turint omenyje, kad asmenys nuolat daro nuotraukas ir filmuoja ir kad biometrinius duomenis galima analizuoti net iš visur įrengtų AVSS, tai gali sukelti didelį atgrasomąjį poveikį.

Kitas susirūpinimą keliantis klausimas – platus privačių nuotraukų ir vaizdo įrašų naudojimas, įskaitant galimą netinkamą naudojimą, pvz., denonsavimą. Kadangi netinkamas naudojimas, pavyzdžiui, denonsavimas, taip pat yra rizika, apskritai būdinga baudžiamajam procesui, pavojus yra daug didesnis dėl tvarkomų duomenų apimties ir dalyvaujančių asmenų skaičiaus, nes žmonės gali įkelti ir medžiagą, susijusią su konkrečiu jiems nepatinkančiu asmeniu ar tokių asmenų grupe. Policijos prašymai įkelti nuotraukas ir vaizdo įrašus gali lemti, kad žmonės labai noriai juos įkels, ypač atsižvelgiant į tai, kad tai gali būti įmanoma padaryti anonimiškai arba bent jau nereikalaujant atvykti į policijos nuovadą ir pranešti apie savo tapatybę.

3.4. Išvada

Šiame pavyzdyje nėra konkrečios nuostatos, kuria būtų galima remtis kaip teisiniu pagrindu. Tačiau, net jei būtų pakankamas teisinis pagrindas, būtinumo ir proporcingumo reikalavimai nebūtų tenkinami, taigi būtų neproporcingai varžomos duomenų subjekto teisės į pagarbą privačiam gyvenimui ir asmens duomenų apsaugą pagal Chartiją.

[88] T. y. žmones, turinčius ypatingų veidų atpažinimo gebėjimų. Taip pat žr.: Face Recognition by Metropolitan Police Super-Recognisers, 2016 m. vasario 26 d., DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 4 SCENARIJUS

4.1. Aprašymas

Policija taiko būdą, kaip nustatyti asmenų, įtariamų padarius sunkų nusikaltimą, užfiksuotą AVSS, tapatybę retrospektyviai taikant veido atpažinimo technologiją. Pareigūnas rankiniu būdu atrenka vaizdo medžiagoje, kuri buvo surinkta iš nusikaltimo vietos arba kitur atliekant preliminarų tyrimą, esantį įtariamųjų atvaizdą (-us) ir siunčia jį (juos) kriminalistikos padaliniui. Kriminalistikos padalinys naudoja veido atpažinimo technologiją, kad palygintų šį (šiuos) vaizdą (-us) su asmenų nuotraukomis, kurios anksčiau buvo surinktos policijos duomenų bazėje (vadinamojoje aprašomojoje duomenų bazėje, kurią sudaro įtariamieji ir buvę nuteistieji). Aprašomoji duomenų bazė skirta šiai procedūrai – laikinai ir izoliuotoje aplinkoje – atlikti analizę naudojant veido atpažinimo technologiją, kad būtų galima atlikti atitikčių paieškos procesą. Siekiant kuo labiau sumažinti asmenų, dėl kurių rasta atitikčių, teisių ir interesų suvaržymą, labai nedaug kriminalistikos padalinio darbuotojų turi teisę atlikti faktinės atitikčių paieškos procedūrą, prieiga prie duomenų suteikiama tik tiems pareigūnams, kuriems pavesta tirti konkrečią bylą, o prieš perduodant bet kokius rezultatus už tyrimą atsakingam pareigūnui atliekama rankinė rezultatų kontrolė. Biometriniai duomenys už kontroliuojamos ir izoliuotos aplinkos ribų neperduodami. Tyrime toliau naudojamas tik rezultatas ir nuotrauka (ne biometrinių duomenų šablonas). Darbuotojams rengiami specialūs mokymai apie tokio duomenų tvarkymo taisykles ir procedūras, o visas asmens ir biometrinių duomenų tvarkymas yra pakankamai reglamentuotas nacionalinės teisės aktais.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ įtariamieji, nustatyti panaudojant AVSS įrašus
- Atvaizdo šaltinis: ☒ viešai prieinamos erdvės ☒ internetas
- Ryšys su nusikaltimu: ☒ Tiesioginis laikinis
  ☒ Tiesioginis geografinis
- Informacijos užfiksavimo būdas: ☒ nuotolinis
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms: Taip, būtent: ☒ Susirinkimų laisvei ☒ Žodžio laisvei ☒ įvairioms: __

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☒ specialios paskirties duomenų bazės, susijusios su nusikaltimo sritimi

Algoritmas:

- Duomenų tvarkymo rūšis: ☒ asmens tapatybės nustatymas „1 su daugeliu“

Rezultatai:

- Poveikis: ☒ Tiesioginis (pvz., duomenų subjektas areštuojamas, apklausiamas)
- Automatizuotas sprendimas: ☒ NE

Teisinė analizė:

- Taikytina teisinė sistema: ☒ Tos kompetentingos institucijos tokio duomenų tvarkymo (veido atpažinimas) specialieji nacionalinės teisės aktai

4.2. Taikytina teisinė sistema

Šiuo atveju nacionalinėje teisėje nustatyta, kad biometriniai duomenys gali būti naudojami atliekant kriminalistinę analizę, kai tai būtina siekiant nustatyti įtariamųjų, padariusių sunkų nusikaltimą, tapatybę pagal nuotraukas, esančias aprašomojoje duomenų bazėje. Nacionalinėje teisėje nurodoma,

kokie duomenys gali būti tvarkomi, taip pat asmens duomenų vientisumo ir konfidencialumo apsaugos procedūros ir jų sunaikinimo procedūros, taip suteikiant pakankamas garantijas nuo piktnaudžiavimo ir savivalės rizikos.

4.3. Būtinumas ir proporcingumas

Akivaizdu, kad veido atpažinimas kriminalistinio darbo lygmeniu laiko požiūriu yra efektyvesnis nei atitikčių paieška rankiniu būdu. Atrenkant vaizdus iš anksto rankiniu būdu suvaržymas ribojamas, palyginti su visos vaizdo medžiagos palyginimu su duomenų baze, ir taip išskiriami tik tie asmenys, su kuriais susijęs duomenų tvarkymo tikslas, t. y. kovoti su sunkiais nusikaltimais, ir tik į juos taikomasi. Tačiau vis dar svarbu apsvarstyti, ar atitikčių paiešką galima atlikti rankiniu būdu per pagrįstą laikotarpį, priklausomai nuo konkretaus atvejo. Asmenų, turinčių prieigą prie technologijos ir asmens duomenų, apribojimas sumažina poveikį teisėms į privatumą ir duomenų apsaugą; be to, biometrinių duomenų šablonai vėliau tyrimo metu nesaugomi arba nenaudojami. Rankinė rezultato kontrolė taip pat reiškia, kad sumažėja bet kokių klaidingų teigiamų rezultatų rizika.

4.4. Išvada

Svarbu, kad nacionalinės teisės aktuose būtų numatytas tinkamas teisinis biometrinių duomenų tvarkymo ir nacionalinės duomenų bazės, su kuria atliekamas palyginimas, pagrindas. Šiuo atveju, siekiant apriboti duomenų apsaugos teisių suvaržymą, imtasi kelių priemonių, pavyzdžiui, teisiniame pagrinde nurodytos veido atpažinimo technologijos naudojimo sąlygos, asmenų, turinčių prieigą prie technologijų ir biometrinių duomenų, skaičius, rankinė kontrolė ir kt. Veido atpažinimo technologija gerokai padidinamas policijos kriminalistikos padalinio tiriamojo darbo veiksmingumas, ji grindžiama teisės aktais, pagal kuriuos policija gali tvarkyti biometrinius duomenis, kai tai tikrai būtina, todėl šiose ribose gali būti laikoma teisėtu asmens teisės suvaržymu.

5 5 SCENARIJUS

5.1. Aprašymas

Nuotolinis biometrinis tapatybės nustatymas – situacija, kai asmenų tapatybė nustatoma naudojant biometrinius identifikatorius (veido atvaizdą, eiseną, akies rainelę ir kt.) per atstumą, viešojoje erdvėje ir tęstiniu būdu arba nuolat tikrinant juos pagal duomenų bazėje saugomus (biometrinius) duomenis[89]. Nuotolinis biometrinis tapatybės nustatymas atliekamas tikruoju laiku, jeigu vaizdinės medžiagos įrašymas, palyginimas ir tapatybės nustatymas atliekami be reikšmingo delsimo.

Prieš kiekvieną nuotolinį biometrinį tapatybės nustatymą tikruoju laiku policija sudaro tyrimui svarbių subjektų stebėjimo sąrašą. Jame pateikiami asmenų veidų atvaizdai. Remdamasi žvalgybos duomenimis, leidžiančiais manyti, kad asmenys bus tam tikroje zonoje, pavyzdžiui, prekybos centre ar viešoje aikštėje, policija nusprendžia, kada, kur ir kiek laiko naudoti nuotolinį biometrinį tapatybės nustatymą.

Priemonės taikymo dieną jie vietoje pastato policijos furgoną, veikiantį kaip kontrolės centras, kuriame yra vyresnysis policijos pareigūnas. Furgone yra monitoriai, kuriuose rodomi netoliese esančių AVSS kamerų, įrengtų *ad hoc* arba prijungtų prie jau įrengtų kamerų filmuojamos medžiagos srautų, įrašai. Kai pėstieji eina pro kameras, technologija išskiria veido atvaizdus, paverčia juos biometrinių duomenų šablonais ir palygina su stebimų asmenų sąraše esančių asmenų biometrinių duomenų šablonais.

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

Jei nustatoma, kad stebimų asmenų sąraše esantys asmenys ir pro kameras einantys asmenys gali sutapti, furgone esantiems pareigūnams išsiunčiamas perspėjimas, o šie, jei perspėjimas teigiamas, informuoja vietoje esančius pareigūnus, pvz., per radijo ryšio įrenginį. Tuomet vietoje esantis pareigūnas nuspręs, ar įsikišti, ar prieiti prie asmens arčiau ar galiausiai jį sulaikyti. Priemonės, kurių pareigūnas ėmėsi vietoje, yra registruojamos. Atsargaus patikrinimo atveju surinkta informacija (pvz., apie tai, su kuo asmuo yra, ką jis dėvi ir kokia kryptimi jis eina) išsaugoma.

Nurodytame nacionalinės teisės akte numatyta bendra nuostata, pagal kurią biometrinių duomenų tvarkymas siekiant nustatyti unikalią fizinio asmens tapatybę yra leistinas, jeigu tai tikrai būtina ir jeigu taikomos tinkamos atitinkamo asmens teisių ir laisvių apsaugos priemonės.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ visi asmenys
- Atvaizdo šaltinis: ☒ viešai prieinamos erdvės
- Ryšys su nusikaltimu: ☒ Nebūtinai tiesioginis geografinis ar laikinis ryšys
- Informacijos užfiksavimo būdas: ☒ nuotolinis
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms: Taip, būtent: ☒ Susirinkimų laisvei ☒ Žodžio laisvei ☒ įvairioms
- Turimi papildomi informacijos apie duomenų subjektą šaltiniai:
  ☒ kita: neatmetama (pvz., naudotasi bankomatais ar eita į parduotuves)

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☒ specialios paskirties duomenų bazės, susijusios su nusikaltimo sritimi

Algoritmas:

- Duomenų tvarkymo rūšis: ☒ asmens tapatybės nustatymas „1 su daugeliu“

Rezultatai:

- Poveikis: ☒ Tiesioginis (pvz., duomenų subjektas areštuojamas, apklausiamas)
- Automatizuotas sprendimas: ☒ NE
- Saugojimo trukmė: kol bus nutraukti visi galimi tyrimai

Teisinė analizė:

- Duomenų subjektui teikiamos išankstinės informacijos duomenų rūšis: ☒ Teisėsaugos institucijos svetainėje apskritai
- Taikytina teisinė sistema: ☒ Teisėsaugos direktyva daugiausia perkelta į nacionalinę teisę ☒ Bendrojo pobūdžio nacionalinės teisės aktai dėl biometrinių duomenų naudojimo teisėsaugos institucijose

5.2. Taikytina teisinė sistema

Teisiniai pagrindai, kuriuose tik pakartojama Teisėsaugos direktyvos 10 straipsnio bendroji nuostata, nėra pakankamai aiškūs, kad asmenims būtų tinkamai nurodytos sąlygos ir aplinkybės, kuriomis teisėsaugos institucijos turi teisę naudoti viešose vietose esančių AVSS įrašus jų veido biometrinių duomenų šablonui sukurti ir palyginti su policijos duomenų bazėmis. Todėl šiame scenarijuje nustatyta teisinė sistema neatitinka minimaliųjų reikalavimų, kad galėtų būti teisiniu pagrindu[90].

[90] Tais atvejais, kai vykdant mokslinį projektą, kuriuo siekiama ištirti veido atpažinimo technologijos naudojimą, reikėtų tvarkyti asmens duomenis, tačiau tokiam tvarkymui nebūtų taikoma Teisėsaugos direktyvos 4 straipsnio

5.3. Būtinumas ir proporcingumas

Kuo didesnis suvaržymas, tuo aukštesnė būtinumo ir proporcingumo kartelė. Nuotolinis biometrinis tapatybės nustatymas viešosiose erdvėse turi keletą pasekmių pagrindinėms teisėms.

Scenarijai apima kiekvieno praeinančio asmens stebėseną atitinkamoje viešojoje erdvėje. Todėl tai daro didelį poveikį pagrįstiems gyventojų lūkesčiams būti anonimiškiems viešosiose erdvėse[91]. Tai būtina sąlyga daugeliui demokratinio proceso aspektų, pavyzdžiui, priimant sprendimą prisijungti prie pilietinės asociacijos, lankytis susirinkimuose ir susitikti su įvairių socialinių ir kultūrinių sluoksnių žmonėmis, dalyvauti politiniame proteste ir lankytis įvairiose vietose. Siekiant laisvai susirinkti ir keistis informacija bei idėjomis, labai svarbu, kad viešosiose erdvėse būtų užtikrintas anonimiškumas. Taip išsaugomas nuomonių pliuralizmas, taikių susirinkimų laisvė, asociacijų laisvė ir mažumų apsauga, taip pat remiami įgaliojimų atskyrimo ir stabdžių bei atsvarų sistemos principai. Kenkimas anonimiškumo viešosiose erdvėse koncepcijai gali padaryti piliečiams didelį atgrasomąjį poveikį. Jie gali susilaikyti nuo tam tikro elgesio, kuris jokiu būdu neperžengia laisvos ir atviros visuomenės ribų. Tai turėtų įtakos viešajam interesui, nes demokratinėje visuomenėje būtinas jos piliečių apsisprendimas ir dalyvavimas demokratiniame procese.

Jei tokia technologija taikoma, asmenims tiesiog einant gatve, į metro ar kepyklą paveiktoje zonoje, teisėsaugos institucijos rinks asmens duomenis, įskaitant biometrinius duomenis, ir pagal pirmąjį scenarijų taip pat ims juos ieškoti jų atitikčių policijos duomenų bazėse. Situacija, kai tas pats būtų daroma imant pirštų atspaudus, būtų akivaizdžiai neproporcinga.

Aprėpiamų duomenų subjektų skaičius yra labai didelis, nes paveikiami visi, kurie ėjo per atitinkamą viešąją erdvę. Be to, tokie scenarijai suponuotų automatizuotą masinį biometrinių duomenų tvarkymą, taip pat masinę biometrinių duomenų atitikčių paiešką policijos duomenų bazėse.

Pagal Europos jurisprudenciją masinis stebėjimas draudžiamas (pvz., EŽTT byloje *S. ir Marper prieš Jungtinę Karalystę* konstatuota, kad nesirenkamas biometrinių duomenų saugojimas yra „neproporcingas teisės į privatumą suvaržymas“, nes jis nėra laikomas „būtinu demokratinėje visuomenėje“).

Nuotolinis biometrinis tapatybės nustatymas yra taip glaudžiai susijęs su masiniu stebėjimu, kad patikimų apribojimo priemonių nėra. Jis iš esmės skiriasi nuo stebėjimo vaizdo kameromis, nes galimas vaizdo įrašų naudojimas be biometrinio tapatybės nustatymo jau yra didelis suvaržymas, tačiau kartu ribotas, o panaudojus veido atpažinimo technologiją, jau plačiai paplitusios stebėjimo vaizdo kameromis sistemos, kaip pagrindinio duomenų šaltinio, kokybė pasikeis. Be to, ypač atsižvelgiant į numanomą atgrasomąjį poveikį, galimi jau esamų stebėjimo vaizdo kameromis įrenginių taikymo apribojimai nebus matomi, todėl visuomenė jais nepasitikės.

Policijos institucijoms atliekant nuotolinį biometrinį tapatybės nustatymą visi laikomi potencialiais įtariamaisiais. Tačiau valstybėje, kurioje laikomasi teisinės valstybės principo, piliečiai laikomi nekaltais tol, kol pavyks įrodyti netinkamą elgesį. Šis principas taip pat iš dalies atsispindi Teisėsaugos direktyvoje, kuria pabrėžiama, kad požiūris į nuteistus nusikaltėlius ar įtariamuosius, kiek įmanoma, turi būti skirtingas; tokiu atveju teisėsaugos institucijos turi turėti *„rimtų priežasčių manyti, kad jie*

3 dalis arba Sąjungos teisė, būtų taikomas BDAR. Bandomųjų projektų, po kurių būtų vykdomos teisėsaugos operacijos, atveju Teisėsaugos direktyva vis tiek būtų taikoma.

[91] EDAV atsakymas EP nariams dėl DI technologijos „Clearview“ sukurtos veido atpažinimo mobiliosios programėlės, 2020 m. birželio 10 d., nuoroda: OUT2020-0052.

įvykdė arba rengiasi įvykdyti nusikalstamą veiką“ (Teisėsaugos direktyvos 6 straipsnio a punktas), palyginti su asmenimis, kurie nėra nuteisti ar įtariami įvykdę nusikalstamą veiklą.

Transporto mazguose arba viešosiose erdvėse teisėsaugos institucijoms naudojant technologiją, galinčią nustatyti unikalią vieno asmens tapatybę ir atsekti bei analizuoti jo buvimo vietą ir judėjimą, bus atskleista neskelbtina informacija apie asmenį (net apie jo seksualinius pomėgius, religiją, sveikatos problemas). Dėl to kyla didžiulis neteisėtos prieigos prie duomenų ir jų naudojimo pavojus.

Įdiegus sistemą, kurioje galima atskleisti pačią asmens elgesio ir charakteristikų esmę, sukeliamas stiprus atgrasomasis poveikis. Tai verčia žmones abejoti, ar prisijungti prie tam tikros manifestacijos, ir taip kenkia demokratiniam procesui. Be to, susitikimas ir buvimas viešumoje su tam tikru draugu, kuris žinomas kaip turintis problemų su policija arba besielgiantis tam tikru būdu, gali būti vertinamas kritiškai, nes visa tai pritrauktų sistemos algoritmo, taigi ir teisėsaugos institucijų, dėmesį.

Apsaugoti pažeidžiamus duomenų subjektus, pavyzdžiui, vaikus, neįmanoma. Be to, poveikis daromas asmenims, kurie turi profesinį interesą (ir neretai atitinkamą teisinę pareigą) išlaikyti savo ryšių konfidencialumą, pavyzdžiui, žurnalistams, advokatams ir dvasininkams. Tai, pvz., galėtų lemti šaltinio ir žurnalisto arba fakto, kad asmuo konsultuojasi su advokatu baudžiamosios gynybos srityje, atskleidimą. Problema kyla ne tik atsitiktinėse viešosiose vietose, kur, pvz., susitinka žurnalistai ir jų šaltiniai, bet, savaime suprantama, ir viešosiose erdvėse, į kurias būtina patekti norint šiuo atžvilgiu kreiptis į institucijas ar specialistus ir pasinaudoti jų paslaugomis.

Be to, dėl žmonių nepasitenkinimo tuo, kad naudojama veido atpažinimo technologija, jie gali pakeisti savo elgesį, vengti vietų, kuriose ta technologija taikoma, ir taip pasitraukti iš socialinio gyvenimo ir kultūrinių renginių. Priklausomai nuo veido atpažinimo technologijos diegimo masto, poveikis žmonėms gali būti toks didelis, kad gali paveikti jų galimybę gyventi orų gyvenimą[92].

Todėl yra didelė tikimybė, kad bus paveikta teisės į asmens duomenų apsaugą esmė – neliečiama jos dalis. Svarbūs požymiai (žr. gairių 3.1.3.2 skirsnį) visų pirma yra šie: teisėsaugos institucijos dideliu mastu automatiškai tvarko unikalius žmonių biologinius požymius naudodamos tikėtinumu pagrįstus algoritmus, kurių rezultatai paaiškinami tik iš dalies. Teisių į privatumą ir duomenų apsaugą apribojimai nustatomi neatsižvelgiant į asmens individualų elgesį ar su juo susijusias aplinkybes. Statistiškai beveik visi duomenų subjektai, kuriems toks suvaržymas daro poveikį, yra įstatymų besilaikantys asmenys. Galimybės teikti informaciją duomenų subjektui yra ribotos. Daugeliu atvejų kreiptis į teismą bus galima tik vėliau.

Pasikliovimas sistema, pagrįsta tikėtinumu ir ribotu paaiškinamumu, gali lemti atsakomybės išsklaidymą ir nebuvimą teisių gynimo srityje, taip pat gali paskatinti aplaidumą.

Pritaikius tokią sistemą, kuri gali būti taikoma panaudojant ir esamas AVSS kameras, labai nedidelėmis pastangomis ir asmenims nematant, ja gali būti piktnaudžiaujama ir gali būti sudarytos sąlygos sistemingai ir greitai sudaryti asmenų sąrašus pagal etninę kilmę, lytį, religiją ir kt. Asmens duomenų tvarkymo pagal iš anksto nustatytus kriterijus, pavyzdžiui, asmens buvimo vietą ir maršrutą, principas jau taikomas praktikoje[93] ir yra sietinas su diskriminacija.

---

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

[93] Žr. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais 6 straipsnį ir 2018 m. rugsėjo 12 d. Europos Parlamento

Nuotolinio veido atpažinimo sistemos viešai prieinamose vietose dėl jų jautrumo, išraiškingumo ir tvarkomų duomenų kiekio gali būti netinkamai naudojamos, o tai gali turėti neigiamų pasekmių atitinkamiems asmenims. Tokie duomenys taip pat gali būti lengvai renkami ir naudojami siekiant daryti spaudimą pagrindiniams stabdžių ir atsvarų principo subjektams, pvz., politinei opozicijai, pareigūnams ir žurnalistams.

Galiausiai, veido atpažinimo technologijos sistemos paprastai daro stiprų šališkumo poveikį, susijusį su rase ir lytimi: klaidingai teigiami rezultatai neproporcingai paveikia tam tikrų rasių asmenis ir moteris[94], dėl to atsiranda diskriminacija. Policijos priemonės, kurių imamasi gavus klaidingą teigiamą rezultatą, pavyzdžiui, kratos ir areštai, dar labiau stigmatizuoja šias grupes.

5.4. Išvada

Pirmiau minėti scenarijai, susiję su nuotoliniu biometrinių duomenų tvarkymu viešosiose erdvėse tapatybės nustatymo tikslais, neužtikrina tinkamos konkuruojančių privačiųjų ir viešųjų interesų pusiausvyros, todėl pagal juos neproporcingai varžomos duomenų subjekto teisės pagal Chartijos 7 ir 8 straipsnius.

6 6 SCENARIJUS

6.1. Aprašymas

Privatus subjektas sukuria taikomąją programą, kuria naudojant veido atvaizdai perimami iš interneto, kad būtų sukurta duomenų bazė. Tada naudotojas, pvz., policija, gali įkelti nuotrauką ir, naudojant biometrinį tapatybės nustatymą, taikomoji programa bandys rasti atitiktį su veido atvaizdais arba biometrinių duomenų šablonais savo duomenų bazėje.

Vietos policijos departamentas atlieka į vaizdo įrašą patekusio nusikaltimo tyrimą, kai neįmanoma nustatyti kelių galimų liudytojų ir įtariamųjų tapatybės ieškant surinktos informacijos atitikčių su vidaus duomenų bazėmis ar žvalgybos informacija. Remiantis surinkta informacija, šie asmenys nėra užregistruoti jokioje policijos duomenų bazėje. Policija nusprendžia naudoti pirmiau aprašytą priemonę, kurią teikia privati įmonė, ir nustatyti asmenų tapatybę pagal biometrinius duomenis.

Informacijos šaltinis:

- Duomenų subjektų rūšys: ☒ visi piliečiai (liudytojai) ☒ nuteistieji ☒ įtariamieji
- Atvaizdo šaltinis: ☒ Filmuota vaizdo medžiaga, gauta viešojoje vietoje arba surinkta kitur preliminaraus tyrimo metu
- Ryšys su nusikaltimu: ☒ Nebūtinas
- Informacijos užfiksavimo būdas: ☒ nuotolinis
- Aplinkybės, darančios poveikį kitoms pagrindinėms teisėms: Taip, būtent: ☒ Susirinkimų laisvei ☒ Žodžio laisvei ☒ įvairioms: __

Etaloninė duomenų bazė (su kuria lyginama surinkta informacija):

- Specialumas: ☒ Bendro pobūdžio duomenų bazės, pildomos duomenimis iš interneto

Algoritmas:

ir Tarybos reglamento (ES) 2018/1240, kuriuo sukuriama Europos kelionių informacijos ir leidimų sistema (ETIAS) ir iš dalies keičiami reglamentai (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 ir (ES) 2017/2226, 33 straipsnį.

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

- Duomenų tvarkymo rūšis: ☒ asmens tapatybės nustatymas „1 su daugeliu“

Rezultatai:

- Poveikis ☒ Tiesioginis (pvz., duomenų subjektas areštuojamas, apklausiamas, diskriminacinis elgesys)
- Automatizuotas sprendimas: ☒ NE

Teisinė analizė:

- Duomenų subjektui teikiamos išankstinės informacijos rūšis: ☒ Ne

6.2. Taikytina teisinė sistema

Kai privatus subjektas teikia paslaugą, kuri apima asmens duomenų tvarkymą, kurio tikslą ir priemones nustato jis pats (šiuo atveju – vaizdų iš interneto perėmimas siekiant sukurti duomenų bazę), šis privatus subjektas turi turėti teisinį pagrindą tokiam duomenų tvarkymui. Be to, teisėsaugos institucija, kuri nusprendžia naudotis šia paslauga savo tikslais, turi turėti duomenų tvarkymo, kuriam ji nustato tikslus ir priemones, teisinį pagrindą. Kad teisėsaugos institucija galėtų tvarkyti biometrinius duomenis, turi būti teisinė sistema, kurioje būtų nurodytas tikslas, tvarkytini asmens duomenys, duomenų tvarkymo tikslai ir asmens duomenų vientisumo bei konfidencialumo užtikrinimo procedūros, taip pat jų sunaikinimo procedūros.

Šis scenarijus reiškia, kad masiškai renkami asmens duomenys iš asmenų, kurie nežino, kad jų duomenys renkami. Toks duomenų tvarkymas galėtų būti teisėtas tik labai išimtinėmis aplinkybėmis. Priklausomai nuo to, kur yra duomenų bazė, naudojantis tokia paslauga gali tekti perduoti asmens duomenis ir (arba) specialių kategorijų asmens duomenis už Europos Sąjungos ribų (policijai, pavyzdžiui, „siunčiant“ stebėjimo vaizdo įraše esantį arba kitaip gautą veido atvaizdą), todėl tokiam perdavimui reikalingos ypatingos sąlygos, žr. Teisėsaugos direktyvos 39 straipsnį.

Šiame scenarijuje nėra konkrečių taisyklių, pagal kurias teisėsaugos institucija galėtų tvarkyti duomenis.

6.3. Būtinumas ir proporcingumas

Teisėsaugos institucijos naudojimasis paslauga reiškia, kad asmens duomenimis dalijamasi su privačiu subjektu, kuris naudojasi duomenų baze, kurioje neribotai ir masiškai renkami asmens duomenys. Nėra jokio ryšio tarp surinktų asmens duomenų ir teisėsaugos institucijos siekiamo tikslo. Teisėsaugos institucijos duomenų perdavimas privačiam subjektui taip pat reiškia, kad institucija nekontroliuoja duomenų, kuriuos tvarko privatus subjektas, ir duomenų subjektams labai sunku pasinaudoti savo teisėmis, nes jie nežino, kad jų duomenys tvarkomi tokiu būdu. Taip nustatoma labai aukšta kartelė tiems atvejams, kada toks duomenų tvarkymas galėtų būti vykdomas. Abejotina, ar koks nors tikslas atitiktų direktyvoje nustatytus reikalavimus, nes bet kokios nuo teisių į privatumą ir duomenų apsaugą leidžiančios nukrypti nuostatos ir apribojimai taikomi tik tada, kai tai yra tikrai būtina. Bendras veiksmingumo kovojant su sunkiais nusikaltimais interesas pats savaime negali pateisinti duomenų tvarkymo, kai nesirenkamai kaupiami tokie dideli duomenų kiekiai. Todėl toks duomenų tvarkymas neatitiktų būtinumo ir proporcingumo reikalavimų.

6.4. Išvada

Kadangi nėra aiškių, tikslių ir nuspėjamų taisyklių, atitinkančių direktyvos 4 ir 10 straipsnių reikalavimus, ir įrodymų, kad toks duomenų tvarkymas yra tikrai būtinas numatytiems tikslams pasiekti, galima daryti išvadą, kad šios taikomosios programos naudojimas neatitiktų būtinumo ir

proporcingumo reikalavimų ir reikštų neproporcingą duomenų subjektų teisių į pagarbą privačiam gyvenimui ir asmens duomenų apsaugą pagal Chartiją suvaržymą.