Translations proofread by EDPB Members.

This language version has not yet been proofread.

Pamatnostādnes 05/2022 par sejas atpazīšanas tehnoloģijas izmantošanu tiesībaizsardzības jomā

Versija 2.0

Pieņemts 2023. gada 26. aprīlī

Versijas vēsture

Versija 1.0	2022. gada 12. maijs	Pamatnostādņu pieņemšana sabiedriskai apspriešanai
Versija 2.0	2023. gada 26. aprīlis	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas

Saturs

KOPSAVILKUMS

Arvien vairāk tiesībaizsardzības iestāžu piemēro vai plāno piemērot sejas atpazīšanas tehnoloģiju. To var izmantot, lai **autentificētu** vai **identificētu** personu, un to var izmantot video (piemēram, videonovērošanas sistēmā) vai fotogrāfijās. To var izmantot dažādiem mērķiem, tostarp, lai meklētu personas, kas iekļautas policijas kontrolsarakstos, vai lai uzraudzītu personas pārvietošanos publiskajā telpā.

Sejas atpazīšanas tehnoloģija ir balstīta uz **biometrisko datu apstrādi**, tāpēc tā ietver īpašu kategoriju personas datu apstrādi. Bieži sejas atpazīšanas tehnoloģiju izmanto **mākslīgā intelekta** (MI) vai mašīnmācīšanās komponentus. Lai gan tas ļauj veikt plaša mēroga datu apstrādi, tas arī rada diskriminācijas risku un maldinošus rezultātus. Sejas atpazīšanas tehnoloģiju var izmantot kontrolētās 1:1 situācijās, kā arī lielos pūļos un nozīmīgos transporta mezglos.

Sejas atpazīšanas tehnoloģija ir **jutīgs instruments tiesībaizsardzības iestādēm.** Tiesībaizsardzības iestādes ir izpildiestādes, un tām ir suverēnas pilnvaras. Sejas atpazīšanas tehnoloģija ir tendēta iejaukties pamattiesībās — arī ārpus tiesībām uz personas datu aizsardzību — un var ietekmēt mūsu sociālo un demokrātisko politisko stabilitāti.

Attiecībā uz personas datu aizsardzību tiesībaizsardzības kontekstā **ir jāievēro Tiesībaizsardzības direktīvas** prasības. Noteikti ietvari attiecībā uz sejas atpazīšanas tehnoloģijas izmantošanu ir paredzēts Tiesībaizsardzības direktīvai, jo īpaši Tiesībaizsardzības direktīvas 3. panta 13. punktā (termins "biometriskie dati"), 4. pantā (personas datu apstrādes principi), 8. pantā (apstrādes likumīgums), 10. pantā (īpašu kategoriju personas datu apstrāde) un 11. pantā (automatizēta individuāla lēmumu pieņemšana).

Sejas atpazīšanas tehnoloģijas piemērošana var ietekmēt arī vairākas citas pamattiesības. Tādējādi **ES Pamattiesību harta** (Harta) ir būtiska Tiesībaizsardzības direktīvas interpretācijai, jo īpaši tiesības uz personas datu aizsardzību, kas paredzētas Hartas 8. pantā, kā arī tiesības uz privātumu, kas noteiktas Hartas 7. pantā.

Likumdošanas instrumenti, kas kalpo par juridisko pamatu personas datu apstrādei, tieši iejaucas Hartas 7. un 8. pantā garantētajās tiesībās. Biometrisko datu apstrāde jebkādos apstākļos ir nopietna iejaukšanās pati par sevi. Tas nav atkarīgs no iznākuma, piemēram, pozitīvas atbilstības. Visiem atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, un tajos jārespektē šo tiesību un brīvību būtība.

Juridiskajam pamatam jābūt **pietiekami skaidram** tā, lai sniegtu pilsoņiem pienācīgu norādi par nosacījumiem un apstākļiem, kādos iestādēm ir tiesības izmantot jebkādus datu vākšanas un slepenas novērošanas pasākumus. Ja valsts tiesību aktos vienkārši tiktu transponēta Tiesībaizsardzības direktīvas 10. panta vispārīgā klauzula, tam nebūtu precizitātes un skaidrības.

Pirms valsts likumdevējs izveido jaunu juridisko pamatu jebkāda veida biometrisko datu apstrādei, izmantojot sejas atpazīšanu, būtu **jāapspriežas ar kompetento datu aizsardzības uzraudzības iestādi.**

Likumdošanas instrumentiem ir jābūt piemērotiem, lai sasniegtu attiecīgajā likumdošanā izvirzītos leģitīmos mērķus. **Vispārējas nozīmes mērķis** — lai arī cik fundamentāls tas būtu — pats par sevi neattaisno pamattiesību ierobežojumu. Likumdošanas instrumentiem vajadzētu būt **diferencētiem** un vērstiem uz personām, uz kurām tā attiecas, ņemot vērā mērķi, piemēram, apkarot konkrētus smagus noziegumus. Ja pasākums vispārīgi attiecas uz visām personām bez šādas diferenciācijas, ierobežojuma

vai izņēmuma, tas pastiprina iejaukšanos. Tas arī pastiprina iejaukšanos, ja datu apstrāde aptver ievērojamu iedzīvotāju daļu.

Dati ir jāapstrādā tādā veidā, kas nodrošina ES datu aizsardzības noteikumu un principu piemērojamību un efektivitāti. Pamatojoties uz katru situāciju, **nepieciešamības un samērīguma novērtējumā** ir jānosaka un jāapsver arī visas iespējamās sekas attiecībā uz citām pamattiesībām. Ja dati tiek sistemātiski apstrādāti bez datu subjektu ziņas, tas var radīt **vispārēju pastāvīgas uzraudzības sajūtu**. Tas var radīt ierobežojošu ietekmi attiecībā uz dažām vai visām attiecīgajām pamattiesībām, piemēram, cilvēka cieņu saskaņā ar Hartas 1. pantu, domas, apziņas un reliģijas brīvību saskaņā ar Hartas 10. pantu, vārda brīvību saskaņā ar Hartas 11. pantu, kā arī pulcēšanās un biedrošanās brīvību saskaņā ar Hartas 12. pantu.

Īpašu kategoriju datu, piemēram, biometrisko datu, apstrādi var uzskatīt par "**absolūti nepieciešamu**" (Tiesībaizsardzības direktīvas 10. pants) tikai tad, ja iejaukšanās personas datu aizsardzībā un tās ierobežojumi aprobežojas ar to, kas ir absolūti nepieciešams, t. i., neaizstājams, un izslēdz jebkādu vispārēju vai sistemātisku apstrādi.

Tas, ka datu subjekts ir **acīmredzami publiskojis** fotogrāfiju (Tiesībaizsardzības direktīvas 10. pants), nenozīmē, ka saistītie biometriskie dati, kurus var iegūt no fotogrāfijas ar īpašiem tehniskiem līdzekļiem, tiek uzskatīti par acīmredzami publiskotiem. Pakalpojuma noklusējuma iestatījumi, piemēram, veidņu publiskošana vai izvēles neesamība, piemēram, veidnes tiek publiskotas, bet lietotājs nevar mainīt šo iestatījumu, nekādā veidā nebūtu jāuzskata par acīmredzami publiskotiem datiem.

Ar Tiesībaizsardzības direktīvas 11. pantu izveido sistēmu **automatizētai individuālu lēmumu pieņemšanai**. Sejas atpazīšanas tehnoloģijas izmantošana ietver īpašu datu kategoriju izmantošanu, un tā var novest pie profilēšanas atkarībā no tā, kā un kādam nolūkam sejas atpazīšanas tehnoloģija tiek piemērots. Jebkurā gadījumā saskaņā ar Savienības tiesību aktiem un Tiesībaizsardzības direktīvas 11. panta 3. punktu profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, ir aizliegta.

Tiesībaizsardzības direktīvas 6. pants attiecas uz nepieciešamību nošķirt dažādas datu subjektu kategorijas. Attiecībā uz datu subjektiem, par kuriem nav pierādījumu, kas varētu liecināt par to, ka viņu rīcībai varētu būt saikne, pat netieša vai attālināta, ar likumīgu mērķi saskaņā ar Tiesībaizsardzības direktīvu, visticamāk, nav nekāda iejaukšanās pamatojuma.

Datu minimizēšanas princips (Tiesībaizsardzības direktīvas 4. panta 1. punkta e) apakšpunkts) arī paredz, ka visi video materiāli, kas neattiecas uz apstrādes nolūku, vienmēr būtu jānoņem vai jāanonimizē (piemēram, sapludinot tos bez iespējas ar atpakaļejošu spēku atgūt datus) pirms to izvietošanas.

Datu pārzinim ir rūpīgi jāapsver, kā (vai ja tas var) izpildīt prasības attiecībā uz **datu subjekta tiesībām** pirms jebkādas sejas atpazīšanas tehnoloģijas apstrādes uzsākšanas, jo sejas atpazīšanas tehnoloģija bieži ietver īpašu kategoriju personas datu apstrādi bez jebkādas acīmredzamas mijiedarbības ar datu subjektu.

Datu subjekta tiesību efektīva īstenošana ir atkarīga no tā, vai datu pārzinis pilda savus **informēšanas pienākumus** (Tiesībaizsardzības direktīvas 13. pants). Novērtējot, vai pastāv "īpašs gadījums" saskaņā ar Tiesībaizsardzības direktīvas 13. panta 2. punktu, ir jāņem vērā vairāki faktori, tostarp tas, vai personas dati tiek vākti bez datu subjekta ziņas, jo tas būtu vienīgais veids, kā ļaut datu subjektiem efektīvi īstenot savas tiesības. Ja lēmumu pieņemšana tiek veikta, pamatojoties tikai uz sejas

atpazīšanas tehnoloģiju, tad datu subjekti ir jāinformē par automatizētās lēmumu pieņemšanas iezīmēm.

Attiecībā uz **piekļuves pieprasījumiem**, ja biometriskie dati tiek glabāti un saistīti ar identitāti arī ar burtciparu datiem, saskaņā ar datu minimizācijas principu tam būtu jāļauj kompetentajai iestādei sniegt apstiprinājumu piekļuves pieprasījumam, pamatojoties uz šo burtciparu datu meklēšanu un neuzsākot citu personu biometrisko datu turpmāku apstrādi (t. i., meklējot ar sejas atpazīšanas tehnoloģiju datubāzē).

Riski datu subjektiem ir īpaši nopietni, ja neprecīzi dati tiek glabāti policijas datubāzē un/vai kopīgoti ar citām juridiskām personām. Datu pārzinim attiecīgi **jālabo** uzglabātie dati un sejas atpazīšanas tehnoloģijas sistēmas (sk. arī Tiesībaizsardzības direktīvas 47. apsvērumu).

Tiesības uz **ierobežojumu** kļūst īpaši svarīgas, ja runa ir par sejas atpazīšanas tehnoloģiju (kas balstās uz algoritmu(-iem) un tādējādi nekad neuzrāda galīgo rezultātu) situācijās, kad tiek savākts liels datu apjoms un identifikācijas precizitāte un kvalitāte var atšķirties.

Novērtējums par ietekmi uz datu aizsardzību pirms sejas atpazīšanas tehnoloģijas izmantošanas ir obligāta prasība, sal. Tiesībaizsardzības direktīvas 27. pants. EDAK iesaka publiskot šādu novērtējumu rezultātus vai vismaz Novērtējuma par ietekmi uz datu aizsardzību galvenos konstatējumus un secinājumus kā uzticību un pārredzamību veicinošu pasākumu.

Lielākā daļa sejas atpazīšanas tehnoloģijas ieviešanas un izmantošanas gadījumu ietver būtisku risku datu subjektu tiesībām un brīvībām. Tāpēc iestādei, kas ievieš sejas atpazīšanas tehnoloģiju, pirms sistēmas ieviešanas būtu **jākonsultējas** ar kompetento uzraudzības iestādi.

Ņemot vērā biometrisko datu unikālo raksturu, iestādei, kas īsteno un/vai izmanto sejas atpazīšanas tehnoloģiju, būtu jāpievērš īpaša uzmanība **datu apstrādes drošībai**, saskaņā ar Tiesībaizsardzības direktīvas 29. pantu. Jo īpaši tiesībaizsardzības iestādei būtu jānodrošina, ka sistēma atbilst attiecīgajiem standartiem un īsteno biometrisko veidņu aizsardzības pasākumus. Datu aizsardzības principi un aizsardzības pasākumi ir jāiekļauj tehnoloģijā pirms personas datu apstrādes sākuma. Tāpēc pat tad, ja tiesībaizsardzības iestāde plāno piemērot un izmantot sejas atpazīšanas tehnoloģiju no ārējiem pakalpojumu sniedzējiem, tai ir jānodrošina, piemēram, izmantojot iepirkuma procedūru, ka tiek izmantoti tikai sejas atpazīšanas tehnoloģija, kas balstīti uz **datu aizsardzības principiem pēc būtības un pēc noklusējuma**.

Reģistrēšana (sal. Tiesībaizsardzības direktīvas 25. pants) ir svarīgs aizsardzības pasākums, lai pārbaudītu apstrādes likumību gan iekšēji (t. i., attiecīgā datu pārziņa/apstrādātāja pašuzraudzība), gan ārējās uzraudzības iestādes. Saistībā ar sejas atpazīšanas sistēmām ir ieteicams reģistrēt arī atsauces datubāzes izmaiņas un identifikācijas vai verifikācijas mēģinājumus, tostarp lietotāju, rezultātu un ticamības novērtējumu. Tomēr reģistrēšana ir tikai viens no galvenajiem vispārējā **atbildības principa elementiem** (sal. Tiesībaizsardzības direktīvas 4. panta 4. punkts). Datu pārzinim ir jāspēj pierādīt, ka apstrāde atbilst Tiesībaizsardzības direktīvas 4. panta 1.–3. punktā noteiktajiem datu aizsardzības pamatprincipiem.

EDAK atgādina savu un EDAU kopīgo **aicinājumu aizliegt** dažāda veida apstrādi saistībā ar (1) personu biometrisko identifikāciju no attāluma publiski pieejamās telpās, (2) mākslīgā intelekta atbalstītām sejas atpazīšanas sistēmām, kas, pamatojoties uz biometriskajiem datiem, iedala personas grupās pēc etniskās piederības, dzimuma, kā arī pēc politiskās vai seksuālās orientācijas vai citiem diskriminācijas iemesliem (3) sejas atpazīšanas vai līdzīgu tehnoloģiju izmantošanu, lai izdarītu secinājumus par fiziskas personas emocijām, un (4) personas datu apstrādi tiesībaizsardzības kontekstā, kas balstītos uz

datubāzi, kura tiktu aizpildīta, masveidā un bez izšķirības ievācot personas datus, piemēram, "uzkrājot" fotogrāfijas un sejas attēlus, kas pieejami tiešsaistē.

Galvenais attiecīgo pamattiesību aizsargpasākums ir **efektīva uzraudzība**, ko veic kompetentās datu aizsardzības uzraudzības iestādes. Tādēļ dalībvalstīm ir jānodrošina, ka uzraudzības iestāžu resursi ir atbilstoši un pietiekami, lai tās varētu īstenot savas pilnvaras.

Šīs **pamatnostādnes ir adresētas** tiesību aktu pieņēmējiem ES un valstu līmenī, kā arī tiesībaizsardzības iestādēm un to amatpersonām, kas īsteno un izmanto sejas atpazīšanas tehnoloģijas sistēmas. Personas tiek adresētas tiktāl, ciktāl tās ir ieinteresētas vispār vai kā datu subjekti, jo īpaši attiecībā uz datu subjektu tiesībām.

Pamatnostādņu mērķis ir informēt par konkrētām sejas atpazīšanas tehnoloģijas īpašībām un par piemērojamo tiesisko regulējumu tiesībaizsardzības kontekstā (jo īpaši par Tiesībaizsardzības direktīvu).

- Turklāt tās nodrošina **rīku, lai atbalstītu konkrēta lietošanas gadījuma jutīguma pirmo klasifikāciju** (I pielikums).
- Tajos ir ietverti arī **praktiski norādījumi tiesībaizsardzības iestādēm, kas vēlas iepirkt un ekspluatēt** sejas atpazīšanas tehnoloģijas sistēmu (II pielikums).
- Pamatnostādnēs ir izklāstīti arī vairāki tipiski **izmantošanas gadījumi un uzskaitīti daudzi būtiski apsvērumi**, jo īpaši attiecībā uz nepieciešamības un proporcionalitātes pārbaudi (III pielikums).

1 IEVADS

1. Sejas atpazīšanas tehnoloģiju var izmantot, lai automātiski atpazītu indivīdus, pamatojoties uz viņu seju. Sejas atpazīšanas tehnoloģijas pamatā bieži ir mākslīgais intelekts, piemēram, mašīnmācīšanās tehnoloģijas. Sejas atpazīšanas tehnoloģijas lietojumprogrammas tiek arvien vairāk pārbaudītas un izmantotas dažādās jomās, sākot no individuāla lietojuma līdz privātām organizācijām un valsts pārvaldes izmantošanai. Tiesībaizsardzības iestādes (TI) arī sagaida priekšrocības no sejas atpazīšanas tehnoloģijas izmantošanas. Tā sola risinājumus gan salīdzinoši jauniem izaicinājumiem, piemēram, izmeklēšanām, kas saistītas ar lielu fiksēto pierādījumu apjomu, gan arī jau zināmām problēmām, jo īpaši saistībā ar nepietiekamu darbinieku skaitu novērošanas un meklēšanas uzdevumu veikšanai.

2. Liela daļa no pieaugušās intereses par sejas atpazīšanas tehnoloģiju ir pamatota uz sejas atpazīšanas tehnoloģijas efektivitāti un mērogojamību. Tādējādi rodas trūkumi, kas raksturīgi tehnoloģijai un tās izmantošanai — arī plašā mērogā. Lai gan var būt tūkstošiem personas datu kopu, kas tiek analizētas ar vienu pogas spiedienu, jau nelielas algoritmiskās diskriminācijas vai nepareizas identifikācijas sekas var radīt lielu skaitu personu, kuru uzvedība un ikdienas dzīve tiek smagi ietekmēta. Vēl viens būtisks sejas atpazīšanas tehnoloģijas elements ir personas datu, jo īpaši biometrisko datu, apstrādes apjoms, jo personas datu apstrāde ir iejaukšanās pamattiesībās uz personas datu aizsardzību saskaņā ar Eiropas Savienības Pamattiesību hartas (Harta) 8. pantu.

3. TI sejas atpazīšanas tehnoloģijas piemērošanai būs – un zināmā mērā tai jau ir – nozīmīga ietekme uz personām un cilvēku grupām, tostarp minoritātēm. Šīs sekas būtiski ietekmēs arī to, kā mēs dzīvojam kopā, un mūsu sociālo un demokrātiski politisko stabilitāti, novērtējot plurālisma un politiskās opozīcijas lielo nozīmi. Tiesības uz personas datu aizsardzību bieži vien ir galvenais priekšnoteikums, lai garantētu citas pamattiesības. Sejas atpazīšanas tehnoloģijas piemērošana var ievērojami ietekmēt pamattiesības, kas pārsniedz tiesības uz personas datu aizsardzību.

4. Tāpēc EDAK uzskata, ka ir svarīgi veicināt sejas atpazīšanas tehnoloģijas pastāvīgo integrāciju tiesībaizsardzības jomā, uz kuru attiecas[1] attiecīgi Tiesībaizsardzības direktīva, valstu tiesību akti, ar kuriem to transponē, un sniedz šīs pamatnostādnes. Pamatnostādnes ir paredzētas, lai sniegtu attiecīgu informāciju likumdevējiem ES un valstu līmenī, kā arī tiesībaizsardzības iestādēm un to darbiniekiem, īstenojot un izmantojot sejas atpazīšanas tehnoloģijas sistēmas. Pamatnostādņu darbības joma attiecas tikai uz sejas atpazīšanas tehnoloģiju. Tomēr citi uz biometriju balstīti personas datu apstrādes veidi, ko veic TI, jo īpaši, ja tos apstrādā attālināti, var radīt līdzīgus vai papildu riskus personām, grupām un sabiedrībai. Atkarībā no attiecīgajiem apstākļiem daži šo pamatnostādņu aspekti var kalpot kā noderīgs avots arī šajos gadījumos. Visbeidzot, arī personas, kas ir ieinteresētas vispārīgi vai kā datu subjekti, var atrast svarīgu informāciju, jo īpaši par datu subjektu tiesībām.

5. Pamatnostādnes sastāv no galvenā dokumenta un trim pielikumiem. Galvenajā dokumentā ir izklāstīta tehnoloģija un piemērojamais tiesiskais regulējums. Lai palīdzētu noteikt dažus no galvenajiem aspektiem, pēc kuriem klasificēt pamattiesību aizskāruma smagumu konkrētajā piemērošanas jomā, I pielikumā ir sniegts paraugs. TI, kas vēlas iegādāties un izmantot sejas atpazīšanas tehnoloģijas sistēmu, praktiskus norādījumus var atrast II pielikumā. Atkarībā no sejas atpazīšanas tehnoloģijas piemērošanas jomas var būt svarīgi dažādi apsvērumi. Hipotētisku scenāriju un attiecīgu apsvērumu kopums atrodams III pielikumā.

2 TEHNOLOĢIJA

2.1 Viena biometriskā tehnoloģija, divas atšķirīgas funkcijas

6. Sejas atpazīšana ir varbūtiska tehnoloģija, kas var automātiski atpazīt indivīdus, pamatojoties uz viņu seju, lai autentificētu vai identificētu viņus.

7. Sejas atpazīšanas tehnoloģija ietilpst plašākā biometrisko tehnoloģiju kategorijā. Biometriskie dati ietver visus automatizētos procesus, ko izmanto, lai atpazītu indivīdu, kvantificējot fiziskās, fizioloģiskās vai uzvedības īpašības (pirkstu nospiedumus, varavīksnenes struktūru, balsi, gaitu, asinsvadu modeļus utt.). Šīs pazīmes tiek definētas kā "biometriskie dati", jo tās ļauj vai apstiprina šīs personas unikālu identifikāciju.

8. Tas attiecas uz cilvēku sejām vai, precīzāk, to tehnisko apstrādi, izmantojot sejas atpazīšanas ierīces: uzņemot sejas attēlu (fotogrāfiju vai video), ko sauc par biometrisku "paraugu", ir iespējams iegūt šīs sejas atšķirīgo īpašību digitālu atveidojumu (to sauc par "veidni").

9. Biometriskā veidne ir no biometriskā parauga iegūto unikālo iezīmju digitāls attēlojums, kuru var saglabāt biometriskajā datubāzē[2]. Šai veidnei vajadzētu būt unikālai un specifiskai katrai personai, un principā tā ir pastāvīga laika gaitā[3]. Atpazīšanas posmā ierīce salīdzina šo veidni ar citām veidnēm, kas iepriekš iegūtas vai aprēķinātas tieši no biometriskajiem paraugiem, piemēram, sejām, kas redzamas attēlā, fotogrāfijā vai video materiālā. Tādējādi "sejas atpazīšana" ir divu posmu process: sejas attēla ievākšana un tā pārveidošana par veidni, kam seko šīs sejas atpazīšana, salīdzinot atbilstošo veidni ar vienu vai vairākām citām veidnēm.

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI

[2] Pamatnostādnes par sejas atpazīšanu, Konvencijas Padomdevēja komiteja 108 Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi, Eiropas Padome, 2021. gada jūnijs.

[3] Tas var būt atkarīgs no biometrijas veida un datu subjekta vecuma.

10. Tāpat kā jebkurš biometriskais process, sejas atpazīšana var pildīt divas atšķirīgas funkcijas:

- **personas autentifikāciju**, kuras mērķis ir pārbaudīt, vai persona ir tā, par ko tā sevi uzdod. Šādā gadījumā sistēma salīdzina iepriekš ierakstītu biometrisko veidni vai paraugu (piemēram, kas saglabāts viedkartē vai biometriskajā pasē) ar vienu seju, piemēram, personas, kas ieradusies kontrolpunktā, lai pārbaudītu, vai tā ir viena un tā pati persona. Tāpēc šī funkcionalitāte ir atkarīga no divu veidņu salīdzināšanas. To sauc arī par **pārbaudi** "viens pret vienu".

- personas **identificēšanu**, kuras mērķis ir atrast personu no personu grupas konkrētā apgabalā, attēlā vai datubāzē. Šajā gadījumā sistēmai jāapstrādā katra nofotografētā seja, lai izveidotu biometrisko veidni un pēc tam pārbaudītu, vai tā atbilst sistēmai zināmai personai. Tādējādi šī funkcionalitāte ir atkarīga no viena veidnes parauga salīdzināšanas ar veidņu vai paraugu datubāzi (pamatscenāriju). To sauc arī par identifikāciju "vienu pret daudziem". Piemēram, tā var sasaistīt personas vārda, uzvārda ierakstu (vārds, uzvārds) ar seju, ja tiek veikts salīdzinājums ar datubāzi, kurā ir fotogrāfijas, kas saistītas ar vārdiem un uzvārdiem. Tā var būt arī sekošana kādai personai pūlī, ne vienmēr saistot to ar personas pilsonisko identitāti.

11. Abos gadījumos lietotās sejas atpazīšanas metodes ir balstītas uz aplēsto atbilstību starp veidnēm — salīdzināto veidni un pamatscenāriju(-us). No šāda viedokļa tie ir iespējami: salīdzinājums rada lielāku vai mazāku varbūtību, ka persona patiešām ir autentificējamā vai identificējamā persona; ja šī varbūtība sistēmā pārsniedz noteiktu robežvērtību, ko noteicis sistēmas lietotājs vai izstrādātājs, sistēma pieņem, ka pastāv atbilstība.

12. Lai gan abas funkcijas — autentifikācija un identifikācija — ir atšķirīgas, tās abas attiecas uz biometrisko datu apstrādi, kas saistīta ar identificētu vai identificējamu fizisku personu, un tāpēc tās ir personas datu apstrāde un jo īpaši īpašu kategoriju personas datu apstrāde.

13. Sejas atpazīšana ir daļa no plašāka video attēlu apstrādes metožu spektra. Dažas videokameras var filmēt cilvēkus noteiktā apgabalā, jo īpaši viņu sejas, taču tās nevar izmantot, lai automātiski atpazītu personas. Tas pats attiecas uz vienkāršu fotogrāfiju: kamera nav sejas atpazīšanas sistēma, jo cilvēku fotogrāfijas ir jāapstrādā īpašā veidā, lai iegūtu biometriskos datus.

14. Arī sejas atpazīšana ar tā sauktajām "viedajām" kamerām ne vienmēr ir sejas atzīšanas sistēma. Lai gan arī tās rada svarīgus jautājumus ētikas un efektivitātes ziņā, digitālās metodes, ar kurām nosaka neparastu uzvedību vai vardarbīgus notikumus vai atpazīst sejas emocijas vai pat siluetus, nevar uzskatīt par biometriskām sistēmām, kas apstrādā īpašas personas datu kategorijas, ja to mērķis nav unikāli identificēt personu un ja attiecīgā personas datu apstrāde neietver citas īpašas personas datu kategorijas. Šie piemēri nav pilnībā nesaistīti ar sejas atpazīšanu, un uz tiem joprojām attiecas personas datu aizsardzības noteikumi.[4] Turklāt šāda veida atklāšanas sistēmu var izmantot kopā ar citām sistēmām, kuru mērķis ir identificēt personu un kuras tādējādi tiek uzskatītas par sejas atpazīšanas tehnoloģiju.

15. Atšķirībā no, piemēram, video uztveršanas un apstrādes sistēmām, kam nepieciešama fizisku ierīču uzstādīšana, sejas atpazīšana ir programmatūras funkcionalitāte, ko var ieviest esošajās sistēmās (kamerās, attēlu datubāzēs utt.). Tāpēc šādu funkcionalitāti var savienot vai sasaistīt ar daudzām sistēmām un apvienot ar citām funkcijām. Šādai integrācijai jau esošā infrastruktūrā ir jāpievērš īpaša

[4] Tomēr Tiesībaizsardzības direktīvas 10. pants (vai VDAR 9. pants) ir piemērojams sistēmām, ko izmanto, lai personas, pamatojoties uz to biometriskajiem datiem, iedalītu grupās pēc etniskās piederības, kā arī pēc politiskās vai seksuālās orientācijas vai citām īpašām personas datu kategorijām.

uzmanība, jo tā ir saistīta ar raksturīgiem riskiem, ņemot vērā to, ka sejas atpazīšanas tehnoloģija var būt netraucēta un viegli slēpjama[5].

2.2 Plašs mērķu un lietojumu klāsts

16. Ārpus šo pamatnostādņu darbības jomas un ārpus Tiesībaizsardzības direktīvas darbības jomas sejas atpazīšanu var izmantot visdažādākajiem mērķiem, gan komerciālai izmantošanai, gan sabiedrības drošības vai tiesībaizsardzības apsvērumu risināšanai. To var piemērot daudzos dažādos kontekstos: personiskajās attiecībās starp lietotāju un pakalpojumu (piekļuve lietojumprogrammai), lai piekļūtu konkrētai vietai (fiziskā filtrēšana) vai bez jebkādiem īpašiem ierobežojumiem publiskajā telpā (tiešā sejas atpazīšana). To var piemērot jebkura veida datu subjektam: pakalpojuma klientam, darbiniekam, vienkāršam vērotājam, meklējamai personai vai personai, kas iesaistīta tiesvedībā vai administratīvajā procesā utt. Daži datu izmantošanas veidi jau ir plaši izplatīti un ierasti; citi pašlaik ir eksperimentālā vai spekulatīvā stadijā. Lai gan šīs pamatnostādnes neattiecas uz visiem šādiem lietojumiem un pieteikumiem, EDAK atgādina, ka tās var īstenot tikai tad, ja tās atbilst piemērojamajam tiesiskajam regulējumam un jo īpaši VDAR un attiecīgajiem valsts tiesību aktiem.[6] Pat Tiesībaizsardzības direktīvas kontekstā papildus autentifikācijas vai identifikācijas funkcijām datus, kas apstrādāti, izmantojot sejas atpazīšanas tehnoloģiju, var apstrādāt arī citiem mērķiem, piemēram, kategorizācijai.

17. Konkrētāk, varētu apsvērt iespējamo izmantošanas veidu skalu atkarībā no tā, cik lielā mērā cilvēki kontrolē savus personas datus, kādi efektīvi līdzekļi viņiem ir pieejami, lai īstenotu šādu kontroli, un kādas ir viņu tiesības uz iniciatīvu, lai iedarbinātu un izmantotu šo tehnoloģiju, kādas sekas viņiem varētu rasties (atzīšanas vai neatzīšanas gadījumā) un kāda mēroga apstrāde tiek īstenota. Sejas atpazīšana, pamatojoties uz personas ierīcē (viedkartē, viedtālrunī u. c.) glabātu veidni, kas pieder minētajai personai un ko izmanto autentifikācijai un tikai personīgai lietošanai caur specializētu saskarni, nerada tādus pašus riskus kā, piemēram, izmantošana identifikācijas nolūkos nekontrolētā vidē, aktīvi neiesaistot datu subjektus, kur katras sejas veidne, kas iekļūst uzraudzības zonā, tiek salīdzināta ar veidnēm no plaša populācijas šķērsgriezuma, kas glabājas datubāzē. Starp šīm divām galējībām ir ļoti daudzveidīgs lietojumu spektrs un saistīti jautājumi, kas attiecas uz personas datu aizsardzību.

18. Lai sīkāk ilustrētu kontekstu, kādā sejas atpazīšanas tehnoloģijas pašlaik tiek apspriestas vai īstenotas vai nu autentifikācijas, vai identifikācijas nolūkā, EDAK uzskata, ka ir svarīgi minēt virkni piemēru. Turpmāk minētie piemēri ir tikai aprakstoši, un tos nevajadzētu uzskatīt par jebkāda veida iepriekšēju novērtējumu par to atbilstību ES tiesību aktu kopumam datu aizsardzības jomā.

Sejas atpazīšanas autentifikācijas piemēri

19. Autentifikāciju var izstrādāt tā, lai lietotājiem būtu pilnīga kontrole pār to, piemēram, lai nodrošinātu piekļuvi pakalpojumiem vai lietojumprogrammām tikai mājas apstākļos. Tādējādi viedtālruņu īpašnieki to plaši izmanto, lai atbloķētu savu ierīci, nevis paroles autentifikāciju.

20. Sejas atpazīšanas autentifikāciju var izmantot arī, lai pārbaudītu tās personas identitāti, kura vēlas izmantot publiskus vai privātus trešo personu pakalpojumus. Tādējādi šādi procesi piedāvā veidu, kā izveidot digitālu identitāti, izmantojot mobilo lietotni (viedtālruni, planšetdatoru utt.), ko pēc tam var izmantot, lai piekļūtu tiešsaistes administratīvajiem pakalpojumiem.

[5] Piemēram, kamerās, kas tiek piestiprinātas pie ķermeņa, kuras praksē tiek izmantotas arvien vairāk.
[6] Skatīt arī 2020. gada 29. janvārī pieņemtās EDAK pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces, lai saņemtu papildu norādījumus.

21. Turklāt sejas atpazīšanas autentifikācijas mērķis var būt kontrolēt fizisku piekļuvi vienai vai vairākām iepriekš noteiktām vietām, piemēram, ieejām ēkās vai īpašām robežšķērsošanas vietām. Šī funkcionalitāte, piemēram, tiek īstenota noteiktos apstrādes procesos robežšķērsošanas nolūkā, kad personas seja kontrolpunktā tiek salīdzināta ar personas identitātes dokumentā (pasē vai drošā uzturēšanās atļaujā) saglabāto sejas attēlu.

Sejas atpazīšanas identifikācijas piemēri

22. Identifikāciju var piemērot daudzos, pat daudzveidīgākos veidos. Tie jo īpaši ietver, bet ne tikai, turpmāk minētos lietojumus, kas pašlaik novēroti, izmēģināti vai plānoti ES.

- neidentificētas personas (upura, aizdomās turamā u. c.) identitātes meklēšana fotogrāfiju datubāzē;
- personas pārvietošanās uzraudzība publiskajā telpā; viņa seja tiek salīdzināta ar to cilvēku biometriskajām veidnēm, kuri ceļo vai ir ceļojuši uzraudzītajā apgabalā, piemēram, ja bagāžas daļa ir atstāta novārtā vai pēc nozieguma izdarīšanas;
- rekonstruēt personas ceļojumu un tās turpmāko mijiedarbību ar citām personām, novēloti salīdzinot tos pašus elementus, lai noteiktu, piemēram, kontaktus;
- meklēto personu attālināta biometriskā identifikācija publiskās vietās; visas videoaizsardzības kameru tiešraidē iemūžinātās sejas reāllaikā tiek salīdzinātas ar drošības spēku rīcībā esošo datubāzi;
- cilvēku automātiska atpazīšana attēlā, lai identificētu, piemēram, viņu attiecības sociālā tīklā, kas to izmanto; attēls tiek salīdzināts ar visu to tīkla dalībnieku veidnēm, kuri ir piekrituši šai funkcionalitātei, lai ierosinātu šo attiecību nominālo identifikāciju;
- piekļuve pakalpojumiem, daži bankomāti atpazīst savus klientus, salīdzinot videokameras uzņemtu seju ar bankas rīcībā esošo sejas attēlu datubāzi;
- pasažiera ceļojuma izsekošana noteiktā pārvadājuma posmā. Veidne, kas aprēķināta reāllaikā, jebkurai personai, kura veic pārbaudi pie vārtiem, kas atrodas noteiktos ceļojuma posmos (bagāžas izkāpšanas vietas, iekāpšanas vārti u. c.), tiek salīdzināta ar sistēmā iepriekš reģistrēto personu veidnēm.

23. Papildus sejas atpazīšanas tehnoloģijas izmantošanai tiesībaizsardzības jomā, plašais novēroto lietojumu klāsts noteikti prasa visaptverošas debates un politikas pieeju, lai nodrošinātu konsekvenci un atbilstību ES tiesību aktu kopuma datu aizsardzības jomā.

2.3 Uzticamība, precizitāte un riski datu subjektiem

24. Tāpat kā ikviena tehnoloģija, arī sejas atpazīšana var būt problemātiska, kad runa ir par tās ieviešanu, jo īpaši attiecībā uz tās uzticamību un efektivitāti autentifikācijas vai identifikācijas ziņā, kā arī vispārīgo jautājumu par "avota" datu un sejas atpazīšanas tehnoloģijas apstrādes rezultātu kvalitāti un precizitāti.

25. Šādas tehnoloģiskas problēmas rada īpašus riskus attiecīgajiem datu subjektiem, kas ir vēl jo nozīmīgāki vai nopietnāki tiesībaizsardzības jomā, ņemot vērā iespējamo juridisko vai citu līdzīgu ietekmi uz datu subjektiem, kas tos būtiski ietekmē. Šajā kontekstā šķiet lietderīgi arī uzsvērt, ka sejas atpazīšanas

tehnoloģija ex post izmantošana pati par sevi nav drošāka, jo indivīdiem var sekot līdzi laika gaitā un vietās. Tādējādi ex post izmantošana rada arī īpašus riskus, kas jāizvērtē katrā gadījumā atsevišķi[7].

26. Kā savā 2019. gada ziņojumā norādījusi ES Pamattiesību aģentūra, "noteikt nepieciešamo sejas atpazīšanas programmatūras precizitātes līmeni ir sarežģīti: pastāv daudz dažādu veidu, kā novērtēt un izvērtēt precizitāti, arī atkarībā no uzdevuma, mērķa un izmantošanas konteksta. Piemērojot tehnoloģiju vietās, ko apmeklē miljoniem cilvēku, piemēram, dzelzceļa stacijās vai lidostās, salīdzinoši neliela daļa kļūdu (piemēram, 0,01 %)[8] joprojām nozīmē, ka simtiem cilvēku tiek nepareizi atzīmēti. Turklāt, kā aprakstīts 3. sadaļā, dažas cilvēku kategorijas var būt neatbilstīgākas nekā citas. Pastāv dažādi veidi, kā aprēķināt un interpretēt kļūdu biežumu, tāpēc ir nepieciešama piesardzība. Turklāt, runājot par precizitāti un kļūdām, īpaši tiesībaizsardzības nolūkos ir svarīgi jautājumi par to, cik viegli sistēmu var apmānīt, piemēram, ar viltotiem sejas attēliem (tā saukto "izlikšanos")."[9]

27. Šajā kontekstā EDAK uzskata, ka ir svarīgi atgādināt, ka sejas atpazīšanas tehnoloģija neatkarīgi no tā, vai to izmanto autentifikācijas vai identifikācijas nolūkos, nenodrošina galīgu rezultātu, bet paļaujas uz varbūtību, ka divas sejas vai sejas attēli atbilst vienai un tai pašai personai.[10] Šis rezultāts vēl vairāk pasliktinās, ja sejas atpazīšanai ievadīto biometrisko paraugu kvalitāte ir zema. Ievades attēlu miglainums, zema kameras izšķirtspēja, kustības un zema gaisma var būt zemas kvalitātes faktori. Citi aspekti, kas būtiski ietekmē rezultātus, ir izplatība un viltojumi, piemēram, kad noziedznieki cenšas vai nu izvairīties no kamerām, vai arī apmānīt sejas atpazīšanas tehnoloģiju. Daudzos pētījumos ir arī uzsvērts, ka šādi algoritmiskās apstrādes statistiskie rezultāti var būt arī neobjektīvi, jo īpaši avota datu kvalitātes, kā arī mācību datubāzu vai citu faktoru, piemēram, izvietošanas vietas izvēles, dēļ. Turklāt būtu jāuzsver arī sejas atpazīšanas tehnoloģijas ietekme uz citām pamattiesībām, piemēram, privātās un ģimenes dzīves neaizskaramību, vārda un informācijas brīvību, pulcēšanās un biedrošanās brīvību utt.

28. Tādēļ ir būtiski, lai sejas atzīšanas tehnoloģijas uzticamība un precizitāte tiktu ņemta vērā kā kritēriji, lai novērtētu atbilstību galvenajiem datu aizsardzības principiem, kā noteikts Tiesībaizsardzības direktīvas 4. pantā, un jo īpaši attiecībā uz taisnīgumu un precizitāti.

29. Uzsverot, ka augstas kvalitātes datiem ir būtiska nozīme augstas kvalitātes algoritmu izstrādē, EDAK arī uzsver, ka datu pārziņiem, pildot savu atbildības pienākumu, ir jāveic regulāra un sistemātiska algoritmiskās apstrādes novērtēšana, lai jo īpaši nodrošinātu šādas personas datu apstrādes rezultātu precizitāti, godīgumu un ticamību. Personas datus, ko izmanto sejas atpazīšanas tehnoloģijas sistēmu novērtēšanas, apmācības un turpmākas izstrādes nolūkos, drīkst apstrādāt, tikai pamatojoties uz pietiekamu juridisko pamatu un saskaņā ar kopējiem datu aizsardzības principiem.

3 PIEMĒROJAMAIS TIESISKAIS REGULĒJUMS

30. Sejas atpazīšanas tehnoloģiju izmantošana ir nesaraujami saistīta ar personas datu, tostarp īpašu kategoriju datu, apstrādi. Turklāt tai ir tieša vai netieša ietekme uz vairākām pamattiesībām, kas nostiprinātas ES Pamattiesību hartā. Tas ir īpaši svarīgi tiesībaizsardzības un krimināltiesību jomā.

[7] Skatīt III pielikumā sniegtos piemērus.

[8] Šis precizitātes rādītājs izriet no citētā ziņojuma un atspoguļo līmeni, kas daudz labāks nekā pašreizējais algoritmu sniegums sejas atpazīšanas tehnoloģijas lietojumos.

[9] Sejas atpazīšanas tehnoloģija: pamattiesību apsvērumi tiesībaizsardzības kontekstā, ES Pamattiesību aģentūra, 2019. gada 21. novembris.

[10] Šo varbūtību dēvē par “ticamības novērtējumu”.

Tāpēc jebkāda sejas atpazīšanas tehnoloģiju izmantošana būtu jāveic, stingri ievērojot piemērojamo tiesisko regulējumu.

31. Turpmāk sniegto informāciju ir paredzēts izmantot, izvērtējot turpmākos likumdošanas un administratīvos pasākumus, kā arī īstenojot spēkā esošo likumdošanu katrā atsevišķā gadījumā, kas saistīts ar sejas atpazīšanas tehnoloģiju. Attiecīgo prasību būtiskums mainās atkarībā no konkrētajiem apstākļiem. Tā kā nav iespējams paredzēt visus turpmākos apstākļus, tiek uzskatīts, ka tas ir tikai atbalsts un nav interpretējams kā izsmeļošs uzskaitījums.

3.1 Vispārējais tiesiskais regulējums — ES Pamattiesību harta un Eiropas Cilvēktiesību konvencija (ECTK)

3.1.1 Hartas piemērojamība

32. ES Pamattiesību harta (turpmāk — Harta) ir adresēta Savienības iestādēm, struktūrām, birojiem un aģentūrām, kā arī dalībvalstīm, kad tās īsteno Savienības tiesību aktus.

33. Regulējot biometrisko datu apstrādi tiesībaizsardzības nolūkos saskaņā ar Tiesībaizsardzības direktīvas 1. panta 1. punktu, neizbēgami rodas jautājums par atbilstību pamattiesībām, jo īpaši tiesībām uz privātās dzīves un saziņas neaizskaramību saskaņā ar Hartas 7. pantu un tiesībām uz personas datu aizsardzību saskaņā ar Hartas 8. pantu.

34. Fizisku personu, tostarp viņu seju, videoierakstu ievākšana un analīze nozīmē personas datu apstrādi. Veicot attēla tehnisko apstrādi, apstrāde aptver arī biometriskos datus. Datu, kas attiecas uz fiziskas personas sejas vaibstiem, tehniskā apstrāde saistībā ar laiku un vietu ļauj izdarīt secinājumus par attiecīgo personu privāto dzīvi. Šie secinājumi var attiekties uz šo personu rasi vai etnisko izcelsmi, veselību, reliģisko piederību, ikdienas dzīves paradumiem, pastāvīgo vai pagaidu dzīvesvietu, ikdienas vai cita veida pārvietošanos, veiktajām darbībām, sociālajām attiecībām un sociālo vidi, kurā tās uzturas. Plašais informācijas klāsts, kas var tikt atklāts, piemērojot sejas atpazīšanas tehnoloģiju, skaidri parāda iespējamo ietekmi uz tiesībām uz personas datu aizsardzību, kas noteiktas Hartas 8. pantā, kā arī uz tiesībām uz privātumu, kas noteiktas Hartas 7. pantā.

35. Šādos apstākļos nav arī izslēgts, ka attiecīgo biometrisko (sejas) datu ievākšana, analīze un turpmāka apstrāde varētu ietekmēt to, kā cilvēki jūtas brīvi rīkoties, pat ja darbība pilnībā ietilptu brīvas un atvērtas sabiedrības kompetencē. Tas varētu arī nopietni ietekmēt viņu pamattiesību īstenošanu, piemēram, tiesības uz domas, apziņas un ticības brīvību, miermīlīgu pulcēšanās brīvību un biedrošanās brīvību saskaņā ar Hartas 1., 10., 11. un 12. pantu. Šāda apstrāde ietver arī citus riskus, piemēram, attiecīgo iestāžu ievāktās personas informācijas ļaunprātīgas izmantošanas risku, īstenojot nelikumīgu piekļuvi personas datiem un to izmantošanu, drošības pārkāpumu u. tml. Šie riski bieži ir atkarīgi no apstrādes un tās apstākļiem, piemēram, nelikumīgas piekļuves un izmantošanas risku policijas darbiniekiem vai citām nepilnvarotām personām. Tomēr daži riski vienkārši ir raksturīgi biometrisko datu unikālajai būtībai. Atšķirībā no adreses vai tālruņa numura datu subjektam nav iespējams mainīt savas unikālās īpašības, piemēram, seju vai varavīksneni. Neatļautas piekļuves vai nejaušas biometrisko datu publicēšanas gadījumā tas novestu pie tā, ka dati tiktu kompromitēti kā paroles vai kriptogrāfijas atslēgas, vai tos varētu izmantot turpmākām neatļautām uzraudzības darbībām, kas kaitē datu subjektam.

3.1.2 Iejaukšanās Hartā noteiktajās tiesībās

36. Biometrisko datu apstrāde jebkādos apstākļos ir nopietna iejaukšanās pati par sevi. Tas nav atkarīgs no iznākuma, piemēram, pozitīvas atbilstības. Apstrāde ir iejaukšanās pat tad, ja biometriskā veidne tiek

nekavējoties dzēsta pēc tam, kad datu salīdzināšana ar policijas datubāzi noved pie informācijas neatbilsmes.

37. Iejaukšanās datu subjektu pamattiesībās var izrietēt no tiesību akta, kura mērķis vai sekas ir attiecīgo pamattiesību ierobežošana[11]. Tas var izrietēt arī no valsts iestādes darbības ar tādu pašu mērķi vai sekām vai pat no privātas struktūras, kurai ar likumu uzticēts īstenot valsts varu un publiskās pilnvaras.

38. Likumdošanas instruments, kas kalpo par juridisko pamatu personas datu apstrādei, tieši iejaucas Hartas 7. un 8. pantā garantētajās tiesībās[12].

39. Biometrisko datu un jo īpaši sejas atpazīšanas tehnoloģijas izmantošana daudzos gadījumos ietekmē arī tiesības uz cilvēka cieņu, ko garantē Hartas 1. pants. Cilvēka cieņa prasa, lai personas netiktu uzskatītas par vienkāršiem priekšmetiem. Sejas atpazīšanas tehnoloģija aprēķina eksistenciālas un ļoti personīgas īpašības, sejas iezīmes mašīnlasāmā formā, lai to izmantotu kā cilvēka numura zīmi vai ID karti, tādējādi objektivizējot seju.

40. Šāda apstrāde var ietekmēt arī citas pamattiesības, piemēram, tiesības saskaņā ar Hartas 10., 11. un 12. pantu, ciktāl ierobežojoša ietekme ir paredzēta vai izriet no attiecīgās tiesībaizsardzības iestāžu videonovērošanas.

41. Turklāt būtu rūpīgi jāapsver arī iespējamie riski, ko rada sejas atpazīšanas tehnoloģiju izmantošana tiesībaizsardzības iestādēs attiecībā uz tiesībām uz taisnīgu tiesu un nevainīguma prezumpciju saskaņā ar Hartas 47. un 48. pantu. Sejas atpazīšanas tehnoloģijas piemērošanas rezultāts, piemēram, atbilsme, var ne tikai novest pie tā, ka persona tiek pakļauta turpmākai policijas darbībai, bet arī būt izšķirošs pierādījums tiesas procesā. Tādējādi sejas atpazīšanas tehnoloģijas trūkumi, piemēram, iespējama neobjektivitāte, diskriminācija vai nepareiza identifikācija ("viltus pozitīvs rezultāts"), var radīt nopietnas sekas arī kriminālprocesā. Turklāt, novērtējot pierādījumus, sejas atpazīšanas tehnoloģijas piemērošanas rezultāts var būt labvēlīgs pat tad, ja ir pierādījumu atspēkojums (“automatizācijas tendence”).

3.1.3 Iejaukšanās pamatojums

42. Saskaņā ar Hartas 52. panta 1. punktu jebkuram pamattiesību un pamatbrīvību īstenošanas ierobežojumam jābūt paredzētam ar likumu un jāievēro šo tiesību un brīvību būtība. Ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Eiropas Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

3.1.3.1 Paredzēts tiesību aktos

43. Hartas 52. panta 1. punktā ir noteikta prasība par īpašu juridisko pamatu. Šim juridiskajam pamatam ir jābūt pietiekami skaidram, lai sniegtu pilsoņiem pietiekamu priekšstatu par nosacījumiem un apstākļiem, kādos iestādes ir pilnvarotas izmantot jebkādus datu vākšanas un slepenas novērošanas pasākumus[13]. Tajā ir pietiekami skaidri jānorāda valsts iestādēm piešķirtās attiecīgās rīcības brīvības apjoms un īstenošanas veids, lai nodrošinātu indivīdiem minimālo aizsardzības pakāpi, kas tiem pienākas saskaņā ar tiesiskuma principu demokrātiskā sabiedrībā[14]. Turklāt likumības nodrošināšanai nepieciešami atbilstoši aizsardzības pasākumi, lai nodrošinātu, ka tiek ievērotas jo īpaši personas

[11] EST, C-219/91 – Ter Voort, RoC 1992 I-05485, 36.f punkts; EST, C-200/96 – Metronome, RoC 1998 I-1953, 28. punkts.
[12] EST, C-594/12, 36. punkts; EST, C-291/12, 23. punkts un turpmākie punkti.
[13] ECT, Shimovolos pret Krieviju, 68. punkts; Vukota-Bojić pret Šveici.
[14] ECT, Piechowicz pret Poliju, 212. punkts.

tiesības saskaņā ar Hartas 8. pantu. Šie principi attiecas arī uz personas datu apstrādi sejas atpazīšanas tehnoloģijas sistēmu novērtēšanas, apmācības un turpmākas izstrādes nolūkos.

44. Ņemot vērā to, ka biometriskie dati, ko apstrādā, lai veiktu fiziskas personas unikālu identifikāciju, ir īpašas datu kategorijas, kas uzskaitītas Tiesībaizsardzības direktīvas 10. pantā, lielākajā daļā gadījumu atšķirīgiem sejas atpazīšanas tehnoloģijas lietojumiem būtu nepieciešams īpašs tiesību akts, kurā precīzi aprakstīts pieteikums un tā izmantošanas nosacījumi. Tas jo īpaši ietver noziedzības veidus un, attiecīgā gadījumā, šo noziegumu smaguma slieksni, lai cita starpā efektīvi izslēgtu sīkos likumpārkāpumus.[15]

3.1.3.2 Pamattiesību uz privātuma neaizskaramību un personas datu aizsardzību, kas noteikta Hartas 7. un 8. pantā, būtība

45. Pamattiesību ierobežojumiem, kas ir būtiski katrai situācijai, joprojām ir jānodrošina, lai tiktu ievērota konkrēto tiesību būtība. Būtība attiecas uz attiecīgo pamattiesību pašu kodolu[16]. Arī cilvēka cieņa ir jārespektē, pat ja tiesības ir ierobežotas[17].

46. Šādas ir pazīmes, kas liecina par iespējamu neaizskaramā kodola pārkāpumu.

- Noteikums, kas nosaka ierobežojumus neatkarīgi no personas individuālās rīcības vai izņēmuma apstākļiem[18].
- Vērsties tiesās nav iespējams vai vēršanās ir apgrūtināta[19].
- Pirms stingra ierobežojuma netiek ņemti vērā attiecīgās personas apstākļi[20].
- Ņemot vērā Hartas 7. un 8. pantā noteiktās tiesības: Papildus plašai saziņas metadatu ievākšanai, zināšanu iegūšana par elektroniskās saziņas saturu varētu pārkāpt šo tiesību būtību[21].
- Ņemot vērā Hartas 7., 8. un 11. pantā noteiktās tiesības: Likumdošana, kas paredz, ka piekļuves tiešsaistes publisko komunikāciju pakalpojumiem pakalpojumu sniedzējiem un mitināšanas pakalpojumu sniedzējiem parasti un bez izšķirības jāsaglabā, citu starpā personas dati, kas attiecas uz šiem pakalpojumiem[22].
- Attiecībā uz Hartas 8. pantā noteiktajām tiesībām: Arī datu aizsardzības un datu drošības pamatprincipu trūkums varētu pārkāpt tiesību būtību[23].

3.1.3.3 Leģitīms mērķis

47. Kā jau skaidrots 3.1.3. punktā, pamattiesību ierobežojumiem ir patiesi jāatbilst Eiropas Savienības atzītiem vispārējas nozīmes mērķiem vai jāatbilst vajadzībai aizsargāt citu personu tiesības un brīvības.

48. Savienība atzīst gan Līguma par Eiropas Savienību 3. pantā minētos mērķus, gan citas intereses, ko aizsargā īpaši Līgumu noteikumi[24], t. i., cita starpā brīvības, drošības un tiesiskuma telpu, noziedzības

[15] Skatīt, piemēram, EST spriedumus lietās C-817/19 "Ligue des droits humains", punkts 151 f, C-207/16 "Ministerio Fiscal", 56. punkts.
[16] EST, C-279/09, RoC 2010 I-13849, 60. punkts.
[17] Paskaidrojumi attiecībā uz Pamattiesību hartu, I sadaļa, paskaidrojums par 1. pantu, OV C 303, 14.12.2007., 17.–35. lpp.
[18] EST, C-601/15, 52. punkts.
[19] EST, C-400/10, RoC 2010 I-08965, 55. punkts.
[20] EST, C-408/03, RoC 2006 I-02647, 68. punkts.
[21] EST — 203/15 — Tele2 Sverige, 101. punkts ar atsauci uz EST — C-293/12 un C-594/12, 39. punkts.
[22] EST, C-512/18, La Quadrature du Net, 209. punkts un turpmākie punkti.
[23] EST — C-594/12, 40. punkts.
[24] Paskaidrojumi attiecībā uz Pamattiesību hartu, I sadaļa, paskaidrojums par 52. pantu, OV C 303, 14.12.2007., 17.–35. lpp.

novēršanu un apkarošanu. Attiecībās ar pārējo pasauli Savienībai būtu jāveicina miers un drošība, kā arī cilvēktiesību aizsardzība.

49. Nepieciešamība aizsargāt citu personu tiesības un brīvības attiecas uz personu tiesībām, ko aizsargā Eiropas Savienības vai tās dalībvalstu tiesību akti. Novērtējums jāveic ar mērķi saskaņot attiecīgo tiesību aizsardzības prasības un panākt taisnīgu līdzsvaru starp tām[25].

3.1.3.4 Nepieciešamības un proporcionalitātes pārbaude

50. Ja runa ir par iejaukšanos pamattiesībās, valsts un Savienības likumdevēja rīcības brīvības apjoms var izrādīties ierobežots. Tas ir atkarīgs no vairākiem faktoriem, tostarp attiecīgās teritorijas, Hartā garantēto attiecīgo tiesību būtības, iejaukšanās veida un smaguma, kā arī no iejaukšanās mērķa[26]. Likumdošanas instrumentiem ir jābūt piemērotiem, lai sasniegtu attiecīgajā likumdošanā izvirzītos leģitīmos mērķus. Turklāt instrumenti nedrīkst pārsniegt to, kas ir piemērots un vajadzīgs, lai sasniegtu šos mērķus[27]. Vispārējas nozīmes mērķis — lai cik fundamentāls tas arī būtu — pats par sevi neattaisno pamattiesību ierobežojumu[28].

51. Saskaņā ar EST pastāvīgo judikatūru atkāpes un ierobežojumi attiecībā uz personas datu aizsardzību ir jāpiemēro tikai tiktāl, ciktāl tas ir absolūti nepieciešams[29]. Tas nozīmē arī to, ka mērķa sasniegšanai nav pieejami mazāk traucējoši līdzekļi. Rūpīgi jāidentificē un jāizvērtē iespējamās alternatīvas, piemēram, atkarībā no konkrētā mērķa — papildu personāls, biežāka policijas uzraudzība vai papildu ielu apgaismojums. Likumdošanas instrumentiem vajadzētu būt diferencētiem un vērstiem uz personām, uz kurām tie attiecas, ņemot vērā mērķi, piemēram, apkarot smagus noziegumus. Ja tas vispārīgi attiecas uz visām personām bez šādas diferenciācijas, ierobežojuma vai izņēmuma, tā pastiprina iejaukšanos[30]. Tā arī pastiprina iejaukšanos, ja datu apstrāde aptver ievērojamu iedzīvotāju daļu[31].

52. Personas datu aizsardzība, kas izriet no Hartas 8. panta 1. punktā skaidri noteiktā pienākuma, ir īpaši svarīga Hartas 7. pantā nostiprinātajām tiesībām uz privātās dzīves neaizskaramību[32]. Likumdošanā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma darbības jomu un piemērošanu, un jānosaka aizsardzības pasākumi, lai personām, kuru dati ir apstrādāti, būtu pietiekamas garantijas, ka tās var efektīvi aizsargāt savus personas datus pret ļaunprātīgas izmantošanas risku un pret jebkādu nelikumīgu piekļuvi šiem datiem vai to izmantošanu[33]. Nepieciešamība pēc šādām garantijām ir vēl jo lielāka gadījumos, kad personas dati tiek apstrādāti automātiski un pastāv būtisks nelikumīgas piekļuves risks datiem[34]. Turklāt iekšējas vai ārējas,

---

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

[26] EST — C-594/12, 47. punkts ar šādiem avotiem: pēc analoģijas attiecībā uz ECTK 8. pantu, Eir. Tiesa H.R., S. un Marper pret Apvienoto Karalisti [GC], nos. 30562/04 un 30566/04, 102. punkts, ECTK 2008-V.

[27] EST — C-594/12, 46. punkts ar šādiem avotiem: lieta C-343/09 Afton Chemical, ES:C:2010:419, 45. punkts; Volker und Markus Schecke un Eifert, ES:C:2010:662, 74. punkts; Lietas C-581/10 un C-629/10 Nelson u.c., ES:C:2012:657, 71. punkts; lieta C-283/11 Sky Österreich ES:C:2013:28, 50. punkts; un lieta C-101/12 Schaieble, ES:C:2013:661, 29. punkts.

[28] EST — C-594/12, 51. punkts.

[29] EST — C-594/12, 52. punkts, ar šādiem avotiem: Lieta C-473/12 IPI, ES:C:2013:715, 39. punkts un tajā minētā judikatūra.

[30] EST — C-594/12, 57. punkts.

[31] EST — C-594/12, 56. punkts.

[32] EST — C-594/12, 53. punkts.

[33] EST — C-594/12, 54. punkts, ar šādiem avotiem: skatīt pēc analoģijas attiecībā uz ECTK 8. pantu, Eir. Tiesa H.R., Liberty u.c. pret Apvienoto Karalisti, 2008. gada 1. jūlijs, Nr. 58243/00, 62. un 63. punkts; Rotaru pret Rumāniju, no 57. līdz 59. punktam, un S. un Marper pret Apvienoto Karalisti, 99. punkts.

[34] EST — C-594/12, 55. punkts, ar šādiem avotiem: skatīt pēc analoģijas attiecībā uz ECTK 8. pantu, S. un Marper pret Apvienoto Karalisti, 103. punkts, un 2013. gada 18. aprīļa M. K. pret Franciju, Nr. 19522/09, 35. punkts.

piemēram, tiesu iestāžu, sejas atpazīšanas tehnoloģijas izvēršanas atļaujas var būt noderīgas arī kā aizsardzības pasākumi, un dažos nopietnas iejaukšanās gadījumos var izrādīties nepieciešama.[35]

53. Paredzētie noteikumi ir jāpielāgo konkrētajai situācijai, piemēram, apstrādāto datu daudzumam, datu[36] būtībai un nelikumīgas piekļuves riskam. Tādēļ ir vajadzīgi noteikumi, kas jo īpaši skaidri un stingri reglamentētu attiecīgo datu aizsardzību un drošību, lai nodrošinātu to pilnīgu integritāti un konfidencialitāti[37].

54. Saistībā ar attiecībām starp datu pārzini un apstrādātāju nebūtu jāļauj apstrādātājiem ņemt vērā tikai ekonomiskus apsvērumus, nosakot drošības līmeni, ko tie piemēro personas datiem; tas varētu apdraudēt pietiekami augstu aizsardzības līmeni[38].

55. Tiesību aktā ir jānosaka materiālie un procesuālie nosacījumi un objektīvi kritēriji, ar kuriem noteikt ierobežojumus kompetento iestāžu piekļuvei datiem un to turpmākai izmantošanai. Lai novērstu, atklātu vai sauktu pie krimināltatbildības, attiecīgie noziedzīgie nodarījumi būtu jāuzskata par pietiekami nopietniem, lai pamatotu šādas iejaukšanās apmēru un smagumu pamattiesībās, kas noteiktas, piemēram, Hartas 7. un 8. pantā[39].

56. Dati ir jāapstrādā tā, lai nodrošinātu ES datu aizsardzības noteikumu piemērojamību un ietekmi, jo īpaši Hartas 8. pantā paredzētos noteikumus, kuros noteikts, ka aizsardzības un drošības prasību ievērošanu kontrolē neatkarīga iestāde. Šādā situācijā var būt svarīga ģeogrāfiskā vieta, kur notiek apstrāde[40].

57. Attiecībā uz dažādiem personas datu apstrādes posmiem būtu jānošķir datu kategorijas, pamatojoties uz to iespējamo lietderību izvirzītā mērķa sasniegšanai vai atkarībā no attiecīgo personu viedokļa[41]. Apstrādes nosacījumu noteikšanai, piemēram, glabāšanas termiņa noteikšanai, jābūt balstītai uz objektīviem kritērijiem, lai nodrošinātu, ka iejaukšanās aprobežojas ar to, kas ir absolūti nepieciešams[42].

58. Pamatojoties uz katru situāciju, nepieciešamības un proporcionalitātes novērtējumā ir jānosaka un jāņem vērā visas sekas, kas ietilpst citu pamattiesību darbības jomā, piemēram, cilvēka cieņa saskaņā ar Hartas 1. pantu, domas, apziņas un ticības brīvība saskaņā ar Hartas 10. pantu, vārda brīvība saskaņā ar Hartas 11. pantu, kā arī pulcēšanās un biedrošanās brīvība saskaņā ar Hartas 12. pantu.

59. Turklāt ir jāuzskata, ka, ja dati tiek sistemātiski apstrādāti bez datu subjektu ziņas, tas var radīt vispārēju koncepciju par pastāvīgu uzraudzību[43]. Tas var radīt ierobežojošu ietekmi attiecībā uz dažām vai visām attiecīgajām pamattiesībām.

60. Lai atvieglotu un īstenotu nepieciešamības un proporcionalitātes novērtējumu likumdošanas pasākumos, kas saistīti ar sejas atzīšanu tiesībaizsardzības jomā, valstu un Savienības likumdevēji varētu izmantot pieejamos praktiskos instrumentus, kas īpaši izstrādāti šim uzdevumam. Jo īpaši varētu

[35] ECT, Szabó un Vissy pret Ungāriju, 73.–77. punkts.
[36] Skat. arī paaugstinātās prasības tehniskajiem un organizatoriskajiem pasākumiem, apstrādājot īpašu kategoriju datus, Tiesībaizsardzības direktīvas 29. panta 1. punktu.
[37] EST — C-594/12, 66. punkts.
[38] EST — C-594/12, 67. punkts.
[39] EST — C-594/12, 60. un 61. punkts.
[40] EST — C-594/12, 68. punkts.
[41] EST — C-594/12, 63. punkts.
[42] EST — C-594/12, 64. punkts.
[43] EST — C-594/12, 37. punkts.

izmantot Eiropas Datu aizsardzības uzraudzītāja sniegto nepieciešamības un proporcionalitātes instrumentu kopumu[44].

3.1.3.5 Hartas 52. panta 3. punkts, 53. pants (aizsardzības līmenis, arī salīdzinājumā ar ECTK aizsardzības līmeni).

61. Saskaņā ar Hartas 52. panta 3. punktu un 53. pantu to Hartas tiesību nozīmei un darbības jomai, kas atbilst ECTK garantētajām tiesībām, jābūt tādai pašai kā ECTK noteiktajām tiesībām. Lai gan jo īpaši attiecībā uz Hartas 7. pantu var atrast ekvivalentu ECTK, tas neattiecas uz Hartas 8. pantu[45]. Hartas 52. panta 3. punkts neliedz Savienības tiesību aktos paredzēt plašāku aizsardzību. Tā kā ECTK nav juridisks instruments, kas ir oficiāli iekļauts ES tiesību aktos, ES likumdošana ir jāpieņem, ņemot vērā Hartas pamattiesības[46].

62. Saskaņā ar ECTK 8. pantu valsts iestāde nedrīkst iejaukties šo tiesību uz privātās un ģimenes dzīves neaizskaramību īstenošanā, izņemot gadījumus, kad tas ir saskaņā ar likumu un tas ir nepieciešams demokrātiskā sabiedrībā valsts drošības, sabiedriskās drošības vai valsts ekonomiskās labklājības interesēs, lai novērstu nekārtības vai noziegumus, aizsargātu veselību vai tikumību vai lai aizsargātu citu personu tiesības un brīvības.

63. ECTK arī nosaka standartus attiecībā uz to, kā var veikt ierobežojumus. Viena no pamatprasībām, papildus tiesiskuma principam, ir paredzamība. Lai sasniegtu paredzamības prasības, tiesību aktiem jābūt formulētiem pietiekami skaidri, lai sniegtu indivīdiem pienācīgu norādi uz apstākļiem, kādos iestādes ir pilnvarotas izmantot šādus instrumentus.[47] Šī prasība ir atzīta EST un ES datu aizsardzības likumā (sal. 3.2.1.1. sadaļa).

64. Sīkāk precizējot ECTK 8. pantā paredzētās tiesības, ir pilnībā jāievēro arī Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi[48]. Tomēr ir jāuzskata, ka šie noteikumi ir tikai minimālais standarts, ņemot vērā spēkā esošos Savienības tiesību aktus.

3.2 Īpašais tiesiskais regulējums — Tiesībaizsardzības direktīva

65. Tiesībaizsardzības direktīvā ir paredzēts konkrēts regulējums attiecībā uz sejas atpazīšanas tehnoloģijas izmantošanu. Pirmkārt, Tiesībaizsardzības direktīvas 3. panta 13. punktā ir definēts termins "biometriskie dati"[49]. Sīkāku informāciju sal. iepriekš minētā 2.1. sadaļa. Otrkārt, 8. panta 2. punktā ir precizēts, ka, lai jebkura apstrāde būtu likumīga, tai — papildus tam, ka tā ir nepieciešama 1. panta 1. punktā minētajiem nolūkiem — ir jābūt reglamentētai valsts tiesību aktos, kuros noteikti vismaz apstrādes mērķi, apstrādājamie personas dati un apstrādes mērķis. Papildu noteikumi, kam ir īpaša nozīme attiecībā uz biometriskajiem datiem, ir Tiesībaizsardzības direktīvas 10. un 11. pants. 10. pants ir jālasa saistībā ar Tiesībaizsardzības direktīvas 8. pantu[50]. Vienmēr būtu jāievēro

[44] Eiropas Datu aizsardzības uzraudzītājs: To instrumentu nepieciešamības novērtēšana, kas ierobežo pamattiesības uz personas datu aizsardzību: Instrumentu kopums (11.4.2017.); Eiropas Datu aizsardzības uzraudzītājs: EDAU Pamatnostādnes par tādu pasākumu samērīguma novērtēšanu, kuri ierobežo pamattiesības uz privātumu un personas datu aizsardzību (19.12.2019.).

[45] EST — C-203/15 — Tele2 Sverige, 129. punkts.

[46] EST — C-311/18, 99. punkts.

[47] Eiropas Cilvēktiesību tiesas spriedums lietā COPLAND pret APVIENOTO KARALISTI, 03.04.2007., pieteikums Nr. 62617/00, 46. punkts.

[48] ETS Nr. 108.

[49] Tiesībaizsardzības direktīvas 3. panta 13. punkts: "Biometriskie dati" ir apzīmē personas datus pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati.

[50] WP258, Atzinums par dažiem galvenajiem Tiesībaizsardzības direktīvas (ES 2016/680) jautājumiem, 7. lpp.

Tiesībaizsardzības direktīvā 4. pantā noteiktie personas datu apstrādes principi, un, izvērtējot iespējamo biometrisko datu apstrādi, izmantojot sejas atpazīšanas tehnoloģiju, būtu jāvadās pēc šiem principiem.

3.2.1 Īpašu kategoriju datu apstrāde tiesībaizsardzības nolūkos

66. Saskaņā ar Tiesībaizsardzības direktīvas 10. pantu īpašu kategoriju datu, piemēram, biometrisko datu, apstrāde ir atļauta tikai tad, ja tas ir absolūti nepieciešams un ja tiek ievērotas atbilstošas datu subjekta tiesību un brīvību garantijas. Turklāt tā ir atļauta tikai tad, ja to atļauj Savienības vai dalībvalsts tiesību akti, lai aizsargātu datu subjekta vai citas fiziskas personas vitāli svarīgas intereses vai ja šāda apstrāde attiecas uz datiem, kurus datu subjekts ir acīmredzami publiskojis. Šī vispārīgā klauzula uzsver īpašo kategoriju datu apstrādes jutību.

3.2.1.1 Atļauts saskaņā ar Savienības vai dalībvalsts tiesību aktiem

67. Attiecībā uz nepieciešamo likumdošanas pasākuma veidu Tiesībaizsardzības direktīvas 33. apsvērumā ir noteikts, ka "ja šajā direktīvā ir atsauce uz dalībvalsts tiesību aktiem, juridisko pamatu vai likumdošanas instrumentu, tas ne vienmēr nozīmē, ka ir vajadzīgs parlamenta pieņemts leģislatīvs akts, neskarot prasības, kas izriet no attiecīgās dalībvalsts konstitucionālās kārtības."[51]

68. Saskaņā ar Hartas 52. panta 1. punktu visiem Hartā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt "noteiktiem tiesību aktos". Tas atbilst formulējumam "saskaņā ar tiesību aktiem" ECTK 8. panta 2. punktā, kas ne tikai nozīmē atbilstību piemērojamiem tiesību aktiem, bet arī attiecas uz šādu tiesību aktu kvalitāti, nosakot, ka tiem jābūt saderīgiem ar tiesiskumu.

69. Turklāt Tiesībaizsardzības direktīvas 33. apsvērumā ir noteikts, ka "tomēr šādam dalībvalsts tiesību aktam, juridiskajam pamatam vai likumdošanas instrumentam vajadzētu būt skaidram un precīzam un tā piemērošanai vajadzētu būt paredzamai personām, uz kurām tie attiecas, kā to paredz Tiesas un Eiropas Cilvēktiesību tiesas judikatūra. Dalībvalsts tiesību aktos, ar ko reglamentē personas datu apstrādi šīs direktīvas darbības jomā, būtu jānosaka vismaz mērķi, apstrādājamie personas dati, apstrādes nolūki, personas datu integritātes un konfidencialitātes saglabāšanas procedūras un to iznīcināšanas procedūras."

70. Valsts tiesību aktiem jābūt formulētiem pietiekami skaidri, lai sniegtu datu subjektiem pienācīgu norādi uz apstākļiem, kādos datu pārziņi ir pilnvaroti izmantot šādus instrumentus. Tas ietver tādus iespējamos apstrādes priekšnosacījumus kā konkrēti pierādījumu veidi, kā arī nepieciešamība saņemt tiesas vai iekšējo atļauju. Attiecīgais tiesību akts var būt tehnoloģiski neitrāls, ciktāl ir pienācīgi ņemti vērā īpašie riski un īpatnības, kas saistīti ar personas datu apstrādi sejas atpazīšanas tehnoloģijas sistēmās. Saskaņā ar Eiropas Savienības Tiesas (EST) un Eiropas Cilvēktiesību tiesas (ECT) Tiesībaizsardzības direktīvu un judikatūru ir patiešām būtiski, lai likumdošanas instrumenti, kuru mērķis ir nodrošināt juridisko pamatu sejas atpazīšanas instrumentam, datu subjektiem būtu paredzami.

71. Likumdošanas instrumentu nevar izmantot kā tiesību aktu, kas atļauj biometrisko datu apstrādi, izmantojot sejas atpazīšanas tehnoloģiju tiesībaizsardzības nolūkos, ja tas ir tikai Tiesībaizsardzības direktīvas 10. panta vispārīgās klauzulas transponēšana.

72. Papildus biometriskajiem datiem Tiesībaizsardzības direktīvas 10. pants reglamentē citu īpašu kategoriju datu apstrādi, piemēram, seksuālo orientāciju, politiskos uzskatus un reliģisko pārliecību,

[51] Apsveramo likumdošanas pasākumu veidam ir jāatbilst ES tiesību aktiem vai valsts tiesību aktiem. Atkarībā no ierobežojuma ietekmes pakāpes valsts līmenī varētu būt nepieciešams konkrēts likumdošanas instruments, ņemot vērā normu līmeni.

tādējādi aptverot plašu apstrādes klāstu. Turklāt šādā noteikumā nebūtu konkrētu prasību, kas norādītu apstākļus un nosacījumus, saskaņā ar kuriem tiesībaizsardzības iestādes būtu pilnvarotas izmantot sejas atpazīšanas tehnoloģiju. Ņemot vērā atsauci uz citiem datu veidiem un nepārprotamo vajadzību pēc īpašām garantijām bez sīkākām specifikācijām, valsts noteikumu, ar kuru valsts tiesību aktos transponē Tiesībaizsardzības direktīvas 10. pantu — ar tikpat vispārīgu un abstraktu formulējumu — nevar izmantot kā juridisko pamatu biometrisko datu apstrādei, kas saistīta ar sejas atpazīšanu, jo tam trūktu precizitātes un paredzamības. Saskaņā ar Tiesībaizsardzības direktīvas 28. panta 2. punktu vai 46. panta 1. punkta c) apakšpunktu, pirms likumdevējs izveido jaunu juridisko pamatu jebkāda veida biometrisko datu apstrādei, izmantojot sejas atpazīšanu, būtu jāapspriežas ar valsts datu aizsardzības uzraudzības iestādi.

3.2.1.2 Obligāti nepieciešams

73. Apstrādi var uzskatīt par "obligāti nepieciešamu" tikai tad, ja iejaukšanās personas datu aizsardzībā un tās ierobežojumi ir ierobežoti līdz obligāti nepieciešamajam[52]. Vārda "obligāti" pievienošana nozīmē, ka likumdevējs ir paredzējis, ka īpašu kategoriju datu apstrāde var notikt tikai saskaņā ar nosacījumiem, kas ir vēl stingrāki par nepieciešamības nosacījumiem (skat. iepriekš 3.1.3.4. punktu). Šī prasība būtu jāinterpretē kā būtisku. Tas līdz absolūtam minimumam ierobežo rīcības brīvību, kas pieļaujama tiesībaizsardzības iestādei nepieciešamības pārbaudē. Saskaņā ar EST iedibināto judikatūru nosacījums par "obligātu nepieciešamību" ir arī cieši saistīts ar prasību pēc objektīviem kritērijiem, lai definētu apstākļus un nosacījumus, saskaņā ar kuriem var veikt apstrādi, tādējādi izslēdzot jebkādu vispārīgu vai sistemātisku apstrādi[53].

3.2.1.3 Apzināti publiskots

74. Novērtējot, vai apstrāde attiecas uz datiem, kurus datu subjekts acīmredzami publisko, būtu jāatgādina, ka fotogrāfija kā tāda netiek sistemātiski uzskatīta par biometriskajiem datiem[54]. Līdz ar to tas, ka datu subjekts ir acīmredzami publiskojis fotogrāfiju, nenozīmē, ka saistītie biometriskie dati, kurus var iegūt no fotogrāfijas ar īpašiem tehniskiem līdzekļiem, tiek uzskatīti par apzināti publiskotiem.

75. Attiecībā uz personas datiem kopumā, lai biometriskos datus varētu uzskatīt par tādiem, ko datu subjekts ir acīmredzami publiskojis, datu subjektam ir apzināti jāpadara biometrisko veidni (nevis tikai sejas attēlu) brīvi pieejamu un publiski pieejamu, izmantojot atklātu avotu. Ja biometriskos datus izpauž trešā persona, nevar uzskatīt, ka datu subjekts tos ir acīmredzami publiskojis.

76. Turklāt nav pietiekami interpretēt datu subjekta rīcību, lai uzskatītu, ka biometriskie dati ir apzināti publiskoti. Piemēram, sociālo tīklu vai tiešsaistes platformu gadījumā EDAK uzskata, ka fakts, ka datu subjekts nav iedarbinājis vai noteicis konkrētas privātuma iezīmes, nav pietiekams, lai uzskatītu, ka šis datu subjekts ir acīmredzami publiskojis savus personas datus un ka šos datus (piemēram, fotogrāfijas) var apstrādāt biometriskās veidnēs un izmantot identifikācijas nolūkos bez datu subjekta piekrišanas. Vispārīgāk runājot, pakalpojuma noklusējuma iestatījumi, piemēram, veidņu publiskošana vai izvēles neesamība, piemēram, veidnes tiek publiskotas bez lietotāja iespējas mainīt šo iestatījumu, nekādā veidā nebūtu jāuzskata par acīmredzami publiskotiem datiem.

---

[52] Konsekventa judikatūra par pamattiesībām uz privātās dzīves neaizskaramību, skat. EST lietas C-73/07 56. punktu (Satakunnan Markkinapörssi un Satamedia); EST, lietas C-92/09 un C-93/09, 77. punkts (Schecke un Eifert); EST — C-594/12, 52. punkts (Digitālās tiesības); EST lieta C-362/14, 92. punkts (Schrems).

[53] EST lieta C-623/17, 78. punkts.

[54] Sal. VDAR 51. apsvērums: "Fotogrāfiju apstrāde nebūtu sistemātiski jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju. "

3.2.2 Automatizēta individuālo lēmumu pieņemšana, tostarp profilēšana

77. Tiesībaizsardzības direktīvas 11. panta 1. punktā ir paredzēts dalībvalstu pienākums vispārēji aizliegt lēmumus, kuru pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas rada nelabvēlīgas juridiskas sekas attiecībā uz datu subjektu vai būtiski to ietekmē. Atkāpjoties no šī vispārējā aizlieguma, šāda apstrāde var būt iespējama tikai tad, ja to atļauj Savienības vai dalībvalsts tiesību akti, kuri attiecas uz datu pārzini un kuros ir paredzētas atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām, vismaz tiesības panākt cilvēka iejaukšanos no datu pārziņa puses. To var izmantot tikai ierobežotā veidā. Šo robežvērtību piemēro parastajām (t. i., nevis īpašajām) personas datu kategorijām. Uz atbrīvojumu saskaņā ar Tiesībaizsardzības direktīvas 11. panta 2. punktu attiecas vēl augstāka robežvērtība un vēl ierobežotāks lietojums. Tajā atkārtoti uzsvērts, ka lēmumi saskaņā ar pirmo punktu nav balstīti uz īpašām datu kategorijām, t. i., jo īpaši biometriskajiem datiem, lai veiktu fiziskas personas unikālu identifikāciju. Atbrīvojumu var paredzēt tikai tad, ja ir ieviesti piemēroti pasākumi, lai aizsargātu datu subjekta tiesības un brīvības, un attiecīgās fiziskās personas leģitīmās intereses. Šis atbrīvojums ir jāinterpretē papildus un ņemot vērā Tiesībaizsardzības direktīvas 10. panta priekšnoteikumus.

78. Atkarībā no sejas atpazīšanas tehnoloģijas sistēmas pat cilvēka iejaukšanās sejas atpazīšanas tehnoloģijas rezultātu izvērtēšanā pati par sevi var nebūt pietiekama garantija, ka tiek ievērotas personu tiesības un jo īpaši tiesības uz personas datu aizsardzību, ņemot vērā iespējamo neobjektivitāti un kļūdu, kas var rasties pašas apstrādes rezultātā. Turklāt cilvēka iejaukšanos var uzskatīt par aizsardzības līdzekli tikai tad, ja persona, kas iejaucas, cilvēka iejaukšanās laikā var kritiski apstrīdēt sejas atpazīšanas tehnoloģijas rezultātus. Ļoti svarīgi ļaut personai saprast sejas atpazīšanas tehnoloģijas sistēmu un tās robežas, kā arī pareizi interpretēt tās rezultātus. Jāizveido arī darba vieta un organizācija, kas neitralizē automatizācijas neobjektivitātes ietekmi un novērš rezultātu nekritisku pieņemšanu, piemēram, laika spiediena, apgrūtinošu procedūru, iespējamas nelabvēlīgas karjeras ietekmes utt. dēļ.

79. Saskaņā ar Tiesībaizsardzības direktīvas 11. panta 3. punktu profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, piemēram, biometriskajiem datiem, ir aizliegta saskaņā ar Savienības tiesību aktiem. Saskaņā ar Tiesībaizsardzības direktīvas 3. panta 4. punktu "profilēšana" ir jebkāda veida automatizēta personas datu apstrāde, kas ietver personas datu izmantošanu konkrētu ar fizisku personu saistītu personisku aspektu izvērtēšanai, jo īpaši, lai analizētu vai prognozētu aspektus, kas saistīti ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgās vēlmes, intereses, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos. Apsverot, vai ir paredzēti piemēroti pasākumi, lai aizsargātu datu subjekta tiesības un brīvības un attiecīgās fiziskās personas likumīgās intereses, ir jāpatur prātā, ka sejas atpazīšanas tehnoloģijas izmantošana var novest pie profilēšanas atkarībā no sejas atpazīšanas tehnoloģijas izmantošanas veida un mērķa. Jebkurā gadījumā saskaņā ar Savienības tiesību aktiem un Tiesībaizsardzības direktīvas 11. panta 3. punktu profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, ir aizliegta.

3.2.3 Datu subjektu kategorijas

80. Tiesībaizsardzības direktīvas 6. pants attiecas uz nepieciešamību nošķirt dažādas datu subjektu kategorijas. Šī atšķirība ir jānosaka, ja tas ir piemērojams un ciktāl tas ir iespējams. Tai ir jāparāda ietekme uz datu apstrādes veidu. No Tiesībaizsardzības direktīvas 6. pantā sniegtajiem piemēriem var secināt, ka personas datu apstrādei parasti jāatbilst nepieciešamības un proporcionalitātes kritērijiem

arī attiecībā uz datu subjektu kategoriju[55]. Turklāt var secināt, ka attiecībā uz datu subjektiem, par kuriem nav pierādījumu, kas varētu liecināt par to, ka to rīcībai varētu būt, pat netieša vai attālināta, saikne ar leģitīmo mērķi saskaņā ar Tiesībaizsardzības direktīvu, visticamāk, nav nekāda pamatojuma par iejaukšanos[56]. Ja nav piemērojama vai iespējama nošķiršana saskaņā ar Tiesībaizsardzības direktīvas 6. pantu, novērtējot iejaukšanās nepieciešamību un samērīgumu, ir stingri jāņem vērā izņēmums no Tiesībaizsardzības direktīvas 6. panta noteikuma. Atšķirība starp dažādām datu subjektu kategorijām šķiet būtiska prasība attiecībā uz personas datu apstrādi, kas ietver sejas atpazīšanu, ņemot vērā arī iespējamas kļūdaini pozitīvas vai kļūdaini negatīvas atbilsmes, kas var būtiski ietekmēt datu subjektus, kā arī izmeklēšanas gaitā.

81. Kā minēts, īstenojot Savienības tiesību aktus, ir jāievēro Eiropas Savienības Pamattiesību hartas noteikumi, sal. Hartas 52. pants. Tāpēc Tiesībaizsardzības direktīvā paredzētais regulējums un kritēriji ir jālasa, ņemot vērā Hartu. ES un tās dalībvalstu tiesību akti nedrīkst būt zemāki par šo pasākumu, un tiem ir jānodrošina Hartas pilnīga ietekme.

3.2.4 Datu subjekta tiesības

82. EDAK jau ir sniegusi norādījumus par datu subjektu tiesībām saskaņā ar VDAR dažādos aspektos[57]. Tiesībaizsardzības direktīva paredz līdzīgas datu subjektu tiesības, un vispārīgi norādījumi par to ir sniegti 29. panta darba grupas atzinumā, ko apstiprinājusi EDAK[58]. Noteiktos apstākļos Tiesībaizsardzības direktīva pieļauj dažus šo tiesību ierobežojumus. Šādu ierobežojumu parametri tiks sīkāk izklāstīti 3.2.4.6. sadaļā. “Leģitīmi datu subjekta tiesību ierobežojumi”.

83. Lai gan visas datu subjekta tiesības, kas uzskaitītas Tiesībaizsardzības direktīvas III nodaļā, protams, attiecas arī uz personas datu apstrādi, izmantojot sejas atpazīšanas tehnoloģiju, turpmākajā nodaļā uzmanība tiks pievērsta dažām tiesībām un aspektiem, par kuriem varētu būt īpaši svarīgi saņemt norādījumus. Turklāt šī nodaļa un tās analīze ir atkarīga no tā, vai attiecīgajai sejas atpazīšanas tehnoloģijas apstrādei ir izpildītas juridiskās prasības, kā aprakstīts iepriekšējā nodaļā.

84. Ņemot vērā personas datu apstrādes veidu, izmantojot sejas atpazīšanas tehnoloģiju (īpašu kategoriju personas datu apstrāde bieži bez jebkādas acīmredzamas mijiedarbības ar datu subjektu), datu pārzinim ir rūpīgi jāapsver, kā (vai ja tas var) izpildīt Tiesībaizsardzības direktīvas prasības pirms jebkādas sejas atpazīšanas tehnoloģijas apstrādes uzsākšanas. Jo īpaši rūpīgi analizējot:

- kas ir datu subjekti (bieži vien rūpīgāk nekā to, kas ir galvenais mērķis apstrādes nolūkā);
- kā datu subjekti tiek informēti par sejas atpazīšanas tehnoloģijas apstrādi (skat. 3.2.4.1. sadaļu);
- to, kā datu subjekti var īstenot savas tiesības (šajā gadījumā var būt īpaši grūti nodrošināt gan informācijas, gan piekļuves tiesības, kā arī tiesības uz labošanu vai ierobežošanu, ja sejas atpazīšanas tehnoloģija tiek izmantota visām pārbaudēm, izņemot pārbaudi "viens pret vienu", tiešā saziņā ar datu subjektu).

3.2.4.1 Darīt datu subjektiem zināmas tiesības un informāciju kodolīgā, saprotamā un viegli pieejamā veidā

85. Sejas atpazīšanas tehnoloģija paredz izaicinājumus, lai nodrošinātu, ka datu subjekti tiek informēti par to, ka tiek apstrādāti viņu biometriskie dati. Tas ir īpaši sarežģīti, ja tiesībaizsardzības iestāde,

[55] Sal. arī EST — C-594/12, 56.–59. punkts.
[56] Sal. arī EST — C-594/12, 58. punkts.
[57] Skat., piemēram, 1/2022 EDAK Pamatnostādnes par datu subjekta tiesībām — piekļuves tiesības un 3/2019 EDAK Pamatnostādnes par personas datu apstrādi, izmantojot videoierīces.
[58] WP258, Atzinums par dažiem galvenajiem Tiesībaizsardzības direktīvas (ES 2016/680) jautājumiem.

izmantojot sejas atpazīšanas tehnoloģiju, analizē videomateriālu, kas iegūts no trešās personas vai ko tai ir sniegusi trešā persona, jo tiesībaizsardzības iestādei ir maz iespēju (un lielākoties to nav vispār) paziņot datu subjektam datu ievākšanas laikā (piemēram, ar norādi uz vietas). Visi videomateriāli, kas neattiecas uz izmeklēšanu (vai apstrādes nolūku), pirms jebkādas biometrisko datu apstrādes veikšanas vienmēr būtu jāizdzēš vai jāanonimizē (piemēram, sapludinot tos bez iespējas atgūt datus ar atpakaļejošu datumu), lai izvairītos no riska, ka nav izpildīts Tiesībaizsardzības direktīvas 4. panta 1. punkta e) apakšpunktā paredzētais minimizācijas princips un Tiesībaizsardzības direktīvas 13. panta 2. punktā noteiktie informēšanas pienākumi. Datu pārziņa pienākums ir novērtēt, kāda informācija datu subjektam būtu svarīga, lai īstenotu savas tiesības, un nodrošinātu, ka tiek sniegta nepieciešamā informācija. Datu subjekta tiesību efektīva īstenošana ir atkarīga no tā, vai datu pārzinis pilda savus informēšanas pienākumus.

86. Tiesībaizsardzības direktīvas 13. panta 1. punktā noteikts, kāda minimālā informācija ir jāsniedz datu subjektam kopumā. Šo informāciju var sniegt pārziņa tīmekļvietnē, drukātā veidā (piemēram, pēc pieprasījuma pieejamā bukletā) vai citos datu subjektam viegli pieejamos avotos. Datu pārzinim jebkurā gadījumā ir jānodrošina, ka informācija tiek efektīvi sniegta attiecībā uz vismaz šādiem elementiem:

- datu pārziņa, tostarp datu aizsardzības speciālista, identitāti un kontaktinformāciju;
- apstrādes nolūku un to, ka apstrāde tiek veikta, izmantojot sejas atpazīšanas tehnoloģiju;
- tiesības iesniegt sūdzību uzraudzības iestādei un šādas iestādes kontaktinformāciju;
- tiesības pieprasīt piekļuvi personas datiem un to labošanu vai dzēšanu un personas datu apstrādes ierobežošanu.

87. Turklāt īpašos gadījumos, kā noteikts valsts tiesību aktos, kam būtu jāatbilst Tiesībaizsardzības direktīvas 13. panta 2. punktam[59], piemēram, attiecībā uz sejas atpazīšanas tehnoloģijas apstrādi, tieši datu subjektam ir jāsniedz šāda informācija:

- apstrādes juridisko pamatu;
- informāciju par to, kur personas dati tika ievākti bez datu subjekta ziņas;
- laikposms, kurā personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, kas izmantoti minētā laikposma noteikšanai,
- attiecīgā gadījumā personas datu saņēmēju kategorijas (tostarp trešās valstis vai starptautiskās organizācijas).

88. Lai gan Tiesībaizsardzības direktīvas 13. panta 1. punkts attiecas uz vispārēju informāciju, kas ir publiski pieejama, Tiesībaizsardzības direktīvas 13. panta 2. punkts attiecas uz papildu informāciju, kas jāsniedz konkrētam datu subjektam īpašos gadījumos, piemēram, ja dati tiek ievākti tieši no datu subjekta vai netieši bez datu subjekta ziņas[60]. Nav skaidras definīcijas par to, kas ir domāts ar "īpašiem gadījumiem" Tiesībaizsardzības direktīvas 13. panta 2. punktā. Tomēr tas attiecas uz situācijām, kad datu subjektiem ir jāinformē par apstrādi, kas attiecas tieši uz viņiem, un jāsaņem atbilstoša informācija, lai viņi varētu efektīvi izmantot savas tiesības. EDAK uzskata, ka, novērtējot, vai pastāv "īpašs gadījums", ir jāņem vērā vairāki faktori, tostarp, ja personas dati tiek ievākti bez datu subjekta ziņas, jo tas būtu vienīgais

[59] piemēram, Vācijas Federālā datu aizsardzības likuma 56. panta 1. punkts, kurā cita starpā noteikts, kāda informācija ir jāsniedz datu subjektiem slepenās operācijās

[60] WP258, Atzinums par dažiem galvenajiem jautājumiem tiesībaizsardzības direktīvā (ES 2016/680), 17.–18. lpp.

veids, kā ļaut datu subjektiem efektīvi īstenot savas tiesības. Citi "īpašu gadījumu" piemēri varētu būt, ja personas dati tiek apstrādāti tālāk kā starptautiskās kriminālās sadarbības procedūras subjekts vai ja personas dati tiek apstrādāti slepenu operāciju ietvaros, kā noteikts valsts tiesību aktos. Turklāt no Tiesībaizsardzības direktīvas 38. apsvēruma izriet, ka gadījumā, ja lēmumu pieņemšana tiek veikta, pamatojoties tikai uz sejas atpazīšanas tehnoloģiju, datu subjekti ir jāinformē par automatizētās lēmumu pieņemšanas iezīmēm. Tas arī norādītu, ka tas ir īpašs gadījums, kad datu subjektam būtu jāsniedz papildu informācija saskaņā ar Tiesībaizsardzības direktīvas 13. panta 2. punktu[61].

89. Visbeidzot, jāatzīmē, ka saskaņā ar Tiesībaizsardzības direktīvas 13. panta 3. punktu dalībvalstis var pieņemt likumdošanas pasākumus, kas ierobežo informācijas sniegšanas pienākumu konkrētos gadījumos, lai sasniegtu noteiktus mērķus. Tas ir piemērojams tiktāl un tik ilgi, ciktāl šāds pasākums ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, pienācīgi ievērojot datu subjekta pamattiesības un likumīgās intereses.

3.2.4.2 Tiesības piekļūt datiem

90. Kopumā datu subjektam ir tiesības saņemt pozitīvu vai negatīvu apstiprinājumu par jebkādu viņa personas datu apstrādi un, ja atbilde ir pozitīva, piekļuvi personas datiem kā tādiem, kā arī papildu informāciju, kā minēts Tiesībaizsardzības direktīvas 14. pantā. Attiecībā uz sejas atpazīšanas tehnoloģiju, ja biometriskie dati tiek glabāti un saistīti ar identitāti arī ar burtciparu datiem, tam vajadzētu ļaut kompetentajai iestādei sniegt apstiprinājumu piekļuves pieprasījumam, pamatojoties uz meklēšanu pēc šiem burtciparu datiem un neveicot citu personu biometrisko datu turpmāku apstrādi (t. i., meklējot ar sejas atpazīšanas tehnoloģiju datubāzē). Jāievēro datu minimizēšanas princips, un būtu jāglabā tikai tie dati, kas ir nepieciešami saistībā ar apstrādes nolūku.

3.2.4.3 Tiesības uz personas datu izlabošanu

91. Tā kā sejas atpazīšanas tehnoloģija nenodrošina absolūtu precizitāti, ir īpaši svarīgi, lai datu pārziņi būtu modri attiecībā uz pieprasījumiem labot personas datus. Tas var notikt arī tad, ja datu subjekts, pamatojoties uz sejas atpazīšanas tehnoloģiju, ir iekļauts neprecīzā kategorijā, piemēram, nepamatoti iekļauts aizdomās turamo kategorijā, pamatojoties uz sākotnējo pieņēmumu par rīcības gaitu videomateriālā. Riski datu subjektiem ir īpaši nopietni, ja šādi neprecīzi dati tiek glabāti policijas datubāzē un/vai kopīgoti ar citām vienībām. Datu pārzinim attiecīgi jākoriģē saglabātie dati un sejas atpazīšanas tehnoloģijas sistēmas, skat. Tiesībaizsardzības direktīvas 47. apsvērumu.

3.2.4.4 Tiesības uz dzēšanu

92. Sejas atpazīšanas tehnoloģija vairumā gadījumu, ja to neizmanto "viens pret vienu" pārbaudei/autentifikācijai, nozīmē liela skaita datu subjektu biometrisko datu apstrādi. Tāpēc ir svarīgi, lai datu pārzinis iepriekš apsvērtu, kur ir noteikti tā mērķa un nepieciešamības ierobežojumi, lai dzēšanas pieprasījumu saskaņā ar Tiesībaizsardzības direktīvas 16. pantu varētu izskatīt bez liekas kavēšanās (jo datu pārzinim cita starpā ir jādzēš personas dati, kas tiek apstrādāti, pārsniedzot to, ko pieļauj piemērojamie tiesību akti saskaņā ar Tiesībaizsardzības direktīvas 4., 8. un 10. pantu).

3.2.4.5 Tiesības uz ierobežošanu

93. Ja datu subjekts apstrīd datu precizitāti un nav iespējams pārliecināties par datu precizitāti (vai ja personas dati ir jāsaglabā, lai iegūtu turpmākus pierādījumus), pārzinim ir pienākums ierobežot minētā datu subjekta personas datus saskaņā ar Tiesībaizsardzības direktīvas 16. pantu. Tas kļūst īpaši svarīgi attiecībā uz sejas atpazīšanas tehnoloģiju (pamatojoties uz algoritmu(-iem) un tādējādi nekad

[61] Jāiegaumē atšķirība starp "darīts pieejams datu subjektam" Tiesībaizsardzības direktīvas 13. panta 1. punktā un "sniegt datu subjektam" Tiesībaizsardzības direktīvas 13. panta 2. punktā. Saskaņā ar Tiesībaizsardzības direktīvas 13. panta 2. punktu datu pārzinim ir jānodrošina, ka informācija nonāk pie datu subjekta, ja tīmekļvietnē publicētā informācija nebūs pietiekama.

nenorādot galīgo rezultātu) situācijās, kad tiek vākti lieli datu apjomi un identifikācijas precizitāte un kvalitāte var atšķirties. Izmantojot sliktas kvalitātes videomateriālu (piemēram, no nozieguma vietas), palielinās viltus pozitīvu rezultātu risks. Turklāt, ja sejas attēli kontrolsarakstā netiek regulāri atjaunināti, tas palielina arī viltus pozitīvu vai viltus negatīvu rezultātu risku. Īpašos gadījumos, kad datus nevar dzēst, jo ir pamatots iemesls uzskatīt, ka dzēšana varētu ietekmēt datu subjekta likumīgās intereses, dati būtu jāierobežo un jāapstrādā tikai tādā nolūkā, kura dēļ tie netika dzēsti (skat. Tiesībaizsardzības direktīvas 47. apsvērumu).

3.2.4.6 Datu subjekta tiesību likumīgi ierobežojumi

94. Attiecībā uz datu pārziņa pienākumiem sniegt informāciju un datu subjektu piekļuves tiesībām ierobežojumi ir pieļaujami tikai tad, ja tie ir noteikti tiesību aktos, kam savukārt ir jābūt nepieciešamam un samērīgam pasākumam demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas pamattiesības un leģitīmās intereses (skat. Tiesībaizsardzības direktīvas 13. panta 3. punktu, 13. panta 4. punktu, 15. pantu un 16. panta 4. punktu). Ja sejas atpazīšanas tehnoloģiju izmanto tiesībaizsardzības nolūkos, var sagaidīt, ka tas tiks izmantots apstākļos, kad tas kaitētu mērķim informēt datu subjektu vai atļaut piekļuvi datiem. Tas attiektos, piemēram, uz policijas izmeklēšanu par noziegumu vai lai aizsargātu valsts drošību vai sabiedrisko drošību.

95. Piekļuves tiesības nenozīmē automātisku piekļuvi visai informācijai, piemēram, krimināllietā, kurā tiek izmantoti personas dati. Alternatīvs piemērs tam, kad var tikt atļauti tiesību ierobežojumi, varētu būt krimināllizmeklēšanas laikā.

3.2.4.7 Tiesību īstenošana ar uzraudzības iestādes starpniecību

96. Gadījumos, kad ir likumīgi ierobežojumi tiesību īstenošanai saskaņā ar Tiesībaizsardzības direktīvas III nodaļu, datu subjekts var pieprasīt datu aizsardzības iestādei īstenot savas tiesības tās vārdā, pārbaudot pārziņa veiktās apstrādes likumību. Datu pārzinim ir jāinformē datu subjekts par iespēju īstenot savas tiesības šādā veidā (skat. Tiesībaizsardzības direktīvas 17. pantu un Tiesībaizsardzības direktīvas 46. panta 1. punkta g) apakšpunktu). Attiecībā uz sejas atpazīšanas tehnoloģiju tas nozīmē, ka datu pārzinim ir jānodrošina, ka ir ieviesti atbilstoši pasākumi, lai šādu pieprasījumu varētu apstrādāt, piemēram, ļaujot meklēt ierakstītos materiālus, ja datu subjekts sniedz pietiekamu informāciju, lai varētu atrast viņa personas datus.

3.2.5 Citas juridiskās prasības un garantijas

3.2.5.1 27. pants Datu aizsardzības ietekmes novērtējums

97. Novērtējums par ietekmi uz datu aizsardzību pirms sejas atpazīšanas tehnoloģijas izmantošanas ir obligāta prasība, jo apstrādes veids, jo īpaši izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes būtību, apjomu, kontekstu un nolūkus, var radīt augstu risku fizisku personu tiesībām un brīvībām. Ņemot vērā, ka sejas atpazīšanas tehnoloģijas izmantošana ir saistīta ar sistemātisku īpašu kategoriju datu automātisku apstrādi, varētu pieņemt, ka šādos gadījumos pārzinim parasti būtu jāveic datu aizsardzības novērtēšana. Novērtējumā par ietekmi uz datu aizsardzību būtu jāietver vismaz vispārējs apraksts par paredzētajām apstrādes darbībām, novērtējums par apstrādes darbību nepieciešamību un samērīgumu saistībā ar nolūkiem, novērtējums par riskiem datu subjektu tiesībām un brīvībām, pasākumi, kas paredzēti minēto risku novēršanai, aizsardzības pasākumi, drošības pasākumi un mehānismi, lai nodrošinātu personas datu aizsardzību un pierādītu atbilstību. EDAK iesaka publiskot šādu novērtējumu rezultātus vai vismaz Novērtējuma par ietekmi uz datu aizsardzību galvenos konstatējumus un secinājumus kā uzticību un pārredzamību veicinošu pasākumu[62].

[62] Sīkāku informāciju skatīt WP248 red.01 Novērtējuma par ietekmi uz datu aizsardzību Pamatnostādnes par Novērtējumu par ietekmi uz datu aizsardzību un noteikšanu, vai apstrāde "var radīt augstu risku".

3.2.5.2 28. pants Iepriekšēja apspriešanās ar uzraudzības iestādi

98. Saskaņā ar Tiesībaizsardzības direktīvas 28. pantu datu pārzinim vai apstrādātājam pirms apstrādes ir jāapspriežas ar uzraudzības iestādi, ja: a) Novērtējums par ietekmi uz datu aizsardzību liecina, ka apstrāde radītu augstu risku, ja datu pārzinis neveiktu pasākumus riska mazināšanai; vai b) apstrādes veids, jo īpaši, ja jaunu tehnoloģiju, mehānismu vai procedūru izmantošana ir saistīta ar augstu risku datu subjektu tiesībām un brīvībām. Kā jau paskaidrots šo pamatnostādņu 2.3. sadaļā, EDAK uzskata, ka lielākā daļa sejas atpazīšanas tehnoloģijas ieviešanas un izmantošanas gadījumu ietver būtisku augstu risku datu subjektu tiesībām un brīvībām. Tāpēc papildus Novērtējumam par ietekmi uz datu aizsardzību, iestādei, kas izvieto sejas atpazīšanas tehnoloģiju, pirms sistēmas ieviešanas būtu jāapspriežas ar kompetento uzraudzības iestādi.

3.2.5.3 29. pants Apstrādes drošība

99. Biometrisko datu unikālā būtība neļauj datu subjektam tos mainīt, ja tie tiek apdraudēti, piemēram, datu aizsardzības pārkāpuma rezultātā. Tādēļ kompetentajai iestādei, kas īsteno un/vai izmanto sejas atpazīšanas tehnoloģiju, būtu jāpievērš īpaša uzmanība apstrādes drošībai saskaņā ar Tiesībaizsardzības direktīvas 29. pantu. Jo īpaši tiesībaizsardzības iestādei būtu jānodrošina sistēmas atbilstība attiecīgajiem standartiem un jāīsteno biometriskās veidnes aizsardzības pasākumi[63]. Šis pienākums ir vēl svarīgāks, ja tiesībaizsardzības iestāde izmanto trešās puses pakalpojumu sniedzēju (datu apstrādātāju).

3.2.5.4 20. pants Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

100. Integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma saskaņā ar Tiesībaizsardzības direktīvas 20. pantu mērķis ir nodrošināt, ka datu aizsardzības principi un aizsardzības pasākumi, piemēram, datu minimizēšana un glabāšanas ierobežojums, ir integrēti tehnoloģijā, izmantojot atbilstīgus tehniskus un organizatoriskus pasākumus, piemēram, pseidonimizāciju, pat pirms personas datu apstrādes sākuma, un tie tiks piemēroti visā tās dzīves ciklā. Ņemot vērā fizisko personu tiesībām un brīvībām piemītošo augsto risku, šādu pasākumu izvēlei nevajadzētu būt atkarīgai tikai no ekonomiskiem apsvērumiem,[64] bet tā vietā būtu jācenšas īstenot jaunākos sasniegumus datu aizsardzības tehnoloģiju jomā. Tāpat, ja tiesībaizsardzības iestāde plāno piemērot un izmantot sejas atpazīšanas tehnoloģiju no ārējiem pakalpojumu sniedzējiem, tai ir jānodrošina, piemēram, izmantojot iepirkuma procedūru, ka tiek izmantota tikai sejas atpazīšanas tehnoloģija, kas balstīta uz datu aizsardzības principiem pēc būtības un pēc noklusējuma[65]. Tas arī nozīmē, ka sejas atpazīšanas tehnoloģijas darbības pārredzamību neierobežo apgalvojumi par komercnoslēpumiem vai intelektuālā īpašuma tiesībām.

3.2.5.5 25. pants Reģistrēšana

101. Tiesībaizsardzības direktīva nosaka dažādas metodes, kā datu pārzinis vai apstrādātājs pierāda apstrādes likumību un nodrošina datu integritāti un datu drošību. Šajā sakarā sistēmu reģistri ir ļoti noderīgs instruments un svarīgs aizsardzības līdzeklis, lai pārbaudītu apstrādes likumību gan iekšēji (t. i., pašuzraudzība), gan ārējās uzraudzības iestādes, piemēram, datu aizsardzības iestādes. Saskaņā ar Tiesībaizsardzības direktīvas 25. pantu reģistra ieraksti par vismaz šādām apstrādes darbībām būtu jāglabā automatizētās apstrādes sistēmās: ievākšana, pārveidošana, aplūkošana, izpaušana, tostarp

[63] Skatīt, piemēram, ISO/IEC 24745 Informācijas drošība, kiberdrošība un privātuma aizsardzība — Biometriskās informācijas aizsardzība.

[64] Skat. Tiesībaizsardzības direktīvas 53. apsvērumu.

[65] Vairāk informācijas skatīt EDAK Pamatnostādnēs par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

nosūtīšana, kombinēšana un dzēšana. Turklāt datu aplūkošanas un izpaušanas žurnāliem būtu jāļauj noteikt šādu darbību pamatojumu, datumu un laiku un, ciktāl iespējams, tās personas identifikāciju, kura aplūkoja vai izpauda personas datus, kā arī šādu personas datu saņēmēju identitāti. Turklāt sejas atpazīšanas sistēmu kontekstā ir ieteicama šādu papildu apstrādes darbību reģistrēšana (daļēji ārpus Tiesībaizsardzības direktīvas 25. panta):

- Atsauces datubāzes izmaiņas (pievienošana, dzēšana vai atjaunināšana). Reģistram būtu jāsaglabā attiecīgā (pievienotā, dzēstā vai atjauninātā) attēla kopija, ja citādi nav iespējams pārbaudīt apstrādes darbību likumību vai iznākumu.

- Identificēšanas vai pārbaudes mēģinājumi, tostarp iznākuma un ticamības vērtējums. Būtu jāpiemēro stingrs minimizēšanas princips, lai žurnālos tiktu saglabāts tikai atsauces datubāzes attēla identifikators, nevis atsauces attēls. Būtu jāizvairās no ievades biometrisko datu reģistrēšanas, izņemot gadījumus, kad tas ir nepieciešams (piemēram, tikai saskaņošanas gadījumos)

- Tā lietotāja ID, kurš pieprasīja identifikācijas vai pārbaudes mēģinājumu.

- Uz visiem personas datiem, kas glabājas sistēmu reģistros, attiecas stingri mērķa ierobežojumi (piemēram, revīzijas), un tos nedrīkst izmantot citiem mērķiem (piemēram, lai varētu joprojām veikt atzīšanu/pārbaudīšanu, tostarp attēlu, kas ir dzēsts no atsauces datubāzēm). Lai nodrošinātu reģistru integritāti, būtu jāpiemēro drošības pasākumi, savukārt ir ļoti ieteicamas automātiskas uzraudzības sistēmas, lai atklātu reģistru ļaunprātīgu izmantošanu. Attiecībā uz atsauces datubāzes ierakstiem sejas attēlu glabāšanas gadījumā drošības pasākumiem vajadzētu būt līdzvērtīgiem atsauces datubāzei. Būtu arī jāievieš automatizēti procesi, lai nodrošinātu reģistru datu saglabāšanas perioda izpildi.

3.2.5.6 4. panta 4. punkts Pārskatabildība

102. Datu pārzinim ir jāspēj pierādīt, ka apstrāde atbilst principiem, kas izklāstīti Tiesībaizsardzības direktīvas 4. panta no 1. līdz 3. punktam, sal. ar 4. panta 4. punkts. Šajā sakarā ļoti svarīga ir sistēmas sistemātiska un atjaunināta dokumentācija (tostarp atjauninājumi, jauninājumi un algoritmiskā apmācība), tehniskie un organizatoriskie pasākumi (tostarp sistēmas veiktspējas uzraudzība un potenciālā cilvēka iejaukšanās) un personas datu apstrāde. Lai pierādītu apstrādes likumību, īpaši svarīgs elements ir reģistrēšana saskaņā ar Tiesībaizsardzības direktīvas 25. pantu (sal. 3.2.5.5. sadaļa). Pārskatatbildības princips attiecas ne tikai uz sistēmu un apstrādi, bet arī uz tādu procesuālo garantiju dokumentēšanu kā nepieciešamības un proporcionalitātes novērtējumi, Novērtējums par ietekmi uz datu aizsardzību, kā arī iekšējas konsultācijas (piemēram, projekta vadības apstiprinājums vai iekšējie lēmumi par ticamības punktu vērtībām) un ārējās apspriešanās (piemēram, datu aizsardzības iestādē). Šajā sakarā II pielikumā ir iekļauti vairāki elementi.

3.2.5.7 47. pants Efektīva uzraudzība

103. Kompetento datu aizsardzības iestāžu efektīva uzraudzība ir viens no svarīgākajiem sejas atpazīšanas tehnoloģijas izmantošanas skarto personu pamattiesību un pamatbrīvību aizsardzības līdzekļiem. Tajā pašā laikā katras datu aizsardzības iestādes nodrošināšana ar nepieciešamajiem cilvēkresursiem, tehniskajiem un finanšu resursiem, telpām un infrastruktūru ir priekšnoteikums, lai tās varētu efektīvi veikt savus uzdevumus un īstenot savas pilnvaras[66]. Vēl svarīgāk nekā pieejamo darbinieku skaits ir ekspertu prasmes, kuriem būtu jāaptver ļoti plašs jautājumu loks — no kriminālizmeklēšanas un policijas sadarbības līdz lielo datu analītikai un mākslīgajam intelektam. Tāpēc dalībvalstīm būtu

[66] Skat. Komisijas paziņojumu "Pirmais ziņojums par to, kā tiek piemērota un darbojas Direktīva par datu aizsardzību tiesībaizsardzības jomā (ES) 2016/680 ("DAT")", COM(2022) 364 final, 3.4.1. lpp.

jānodrošina, ka uzraudzības iestāžu resursi ir piemēroti un pietiekami, lai tās varētu pildīt savas pilnvaras aizsargāt datu subjektu tiesības, un rūpīgi jāseko līdzi jebkādām izmaiņām šajā jomā.[67]

4 SECINĀJUMS

104. Sejas atpazīšanas tehnoloģiju izmantošana ir nesaraujami saistīta ar ievērojama apjoma personas datu, tostarp īpašu kategoriju datu, apstrādi. Sejas dati un, vispārīgāk, biometriskie dati ir pastāvīgi un neatsaucami saistīti ar personas identitāti. Tāpēc sejas atpazīšanas izmantošana tieši vai netieši ietekmē vairākas ES Pamattiesību hartā nostiprinātas pamattiesības un pamatbrīvības, kas var būt plašākas par privātumu un datu aizsardzību, piemēram, cilvēka cieņu, pārvietošanās brīvību, pulcēšanās brīvību, un citas. Tas ir īpaši svarīgi tiesībaizsardzības un krimināltiesību jomā.

105. EDAK saprot tiesībaizsardzības iestāžu nepieciešamību izmantot vislabākos pieejamos rīkus, lai ātri identificētu teroristu uzbrukumu un citu smagu noziegumu veicējus. Tomēr šādi instrumenti būtu jāizmanto, stingri ievērojot piemērojamo tiesisko regulējumu un tikai gadījumos, kad tie atbilst nepieciešamības un proporcionalitātes prasībām, kā noteikts Hartas 52. panta 1. punktā. Turklāt, lai gan modernās tehnoloģijas var būt daļa no risinājuma, tās nekādā gadījumā nav "zelta vidusceļš".

106. Pastāv daži sejas atpazīšanas tehnoloģiju izmantošanas gadījumi, kas rada nepieņemami augstus riskus indivīdiem un sabiedrībai (“sarkanās līnijas”). Šo iemeslu dēļ EDAK un EDAU ir aicinājuši noteikt to vispārēju aizliegumu[68].

107. Jo īpaši personu biometriskā identifikācija no attāluma publiski pieejamās telpās rada augstu risku, ka notiks iejaukšanās personu privātajā dzīvē, un tai nav vietas demokrātiskā sabiedrībā, jo pēc savas būtības tā ir saistīta ar masveida uzraudzību. Tāpat EDAK uzskata, ka ar MI atbalstītas sejas atpazīšanas sistēmas, kas personas, pamatojoties uz viņu biometriju, iedala grupās pēc etniskās piederības, dzimuma, kā arī politiskās vai seksuālās orientācijas, nav saderīgas ar Hartu. Turklāt EDAK ir pārliecināta, ka sejas atpazīšanas vai līdzīgu tehnoloģiju izmantošana, lai izsecinātu fiziskas personas emocijas, ir ļoti nevēlama un būtu jāaizliedz, iespējams, ar dažiem pienācīgi pamatotiem izņēmumiem. Turklāt EDAK uzskata, ka personas datu apstrāde tiesībaizsardzības kontekstā, kas balstītos uz datubāzi, kura tiktu aizpildīta, ievācot personas datus plašā mērogā un nediferencētā veidā, piemēram, izmantojot tiešsaistē pieejamas fotogrāfijas un sejas attēlus, jo īpaši tos, kas darīti pieejami sociālajos tīklos, kā tāda neatbilst stingrajai nepieciešamības prasībai, kas paredzēta Savienības tiesību aktos.

5 PIELIKUMI

I pielikums. Atbalsta modelis

II pielikums. Praktiski norādījumi par sejas atpazīšanas tehnoloģiju projektu pārvaldību tiesībaizsardzības iestādēs

III pielikums. Praktiski piemēri

[67] Skat. EDAK ieguldījumu Eiropas Komisijas Datu aizsardzības tiesībaizsardzības direktīvas (DAT) novērtējumā saskaņā ar 62. panta 14. punktu, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

[68] Skat. EDPB-EDPS Atzinumu 5/2021 par Ierosinājumu Eiropas Parlamenta un Padomes regulai, kurā ir izklāstīti saskaņotie noteikumi par mākslīgo inteliģenci (Mākslīgās inteliģences akts) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

I PIELIKUMS. SCENĀRIJU APRAKSTA VEIDNE

(Ar informācijas kastēm par aspektiem, kas aplūkoti scenārijā)

Pārstrādes apraksts:

- pārstrādes apraksts, konteksts (saistība ar noziegumu), nolūks

Informācijas avots:

- datu subjektu veidi: ☐ visi iedzīvotāji ☐ notiesātie ☐ aizdomās turamie ☐ bērni, ☐ citi neaizsargāti datu subjekti
- Attēla avots: ☐ publiski pieejamas vietas ☐ internets ☐ privāta struktūra ☐ citas personas ☐ citi .....
- Saistība ar noziegumu: ☐ tiešā laika ziņā ☐ netiešā laika ziņā ☐ tieša ģeogrāfiskā atrašanās vieta ☐ netieša ģeogrāfiskā teritorija ☐ nav nepieciešams
- Informācijas iegūšanas veids: ☐ attālināti ☐ kabīnē vai kontrolētā vidē
- Konteksts — ietekme uz citām pamattiesībām:
  ☐ Nē
  Jā, proti, ☐ pulcēšanās brīvība ☐ Vārda brīvība ☐ dažādi:.....
- Iespējas izmantot papildu informācijas avotus par datu subjektu:
  ☐ Personas apliecinošs dokuments ☐ publiskā tālruņa izmantošana ☐ transportlīdzekļa numura zīme ☐ citi .....

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums: ☐ vispārējas nozīmes datubāzes ☐ īpašas datubāzes, kas saistītas ar noziedzības jomu
- Apraksts par to, kā šīs atsauces datubāzes tika aizpildītas (un juridiskais pamats)
- Datubāzes mērķa maiņa (piemēram, privātīpašuma drošība bija galvenais mērķis): ☐ JĀ ☐ NĒ

Algoritms:

- Apstrādes veids: ☐ pārbaude "viens pret vienu" (autentificēšana) ☐ identifikācija "viens pret daudziem"
- Precizitātes apsvērumi
- Tehniskie aizsardzības pasākumi

Rezultāti:

- Ietekme ☐ Tieša (piemēram, datu subjekts var tikt arestēts, nopratināts, diskriminējoša uzvedība)

☐ Netieša (izmanto statistikas modeļiem, nav nopietnu juridisku darbību pret datu subjektiem)

- Automatizēts lēmums: ☐ JĀ ☐ NĒ
- Uzglabāšanas ilgums

Juridiskā analīze:

- Nepieciešamības un samērīguma analīze — nozieguma mērķis/nopietnība/to personu skaits, kuras nav iesaistītas, bet kuras skar apstrāde
- Datu subjektam sniegtās iepriekšējās informācijas veids: ☐ Ieejot konkrētajā teritorijā ☐ Tiesībaizsardzības iestādes tīmekļvietnē kopumā ☐ Tiesībaizsardzības iestādes tīmekļvietnē par konkrēto apstrādi ☐ Cits .....
- Piemērojamais tiesiskais regulējums :

☐ LED galvenokārt pārkopētas valsts tiesību aktos

☐ Vispārīgi valsts tiesību akti par biometrisko datu izmantošanu tiesībaizsardzības iestādēs

☐ Konkrēti valsts tiesību akti par šo apstrādi (sejas atpazīšana) attiecībā uz šo kompetento iestādi

☐ Konkrēti valsts tiesību akti attiecībā uz šo apstrādi (automatizēts lēmums)

Secinājums:

Vispārīgi apsvērumi par to, vai aprakstītā apstrāde, iespējams, ir saderīga ar ES tiesību aktiem (un daži norādījumi par juridiskiem priekšnoteikumiem)

II PIELIKUMS. PRAKTISKI NORĀDĪJUMI PAR SEJAS ATPAZĪŠANAS TEHNOLOĢIJAS PROJEKTU PĀRVALDĪBU TIESĪBAIZSARDZĪBAS IESTĀDĒS

Šajā pielikumā ir sniegti daži papildu praktiski norādījumi tiesībaizsardzības iestādēm, kas plāno uzsākt projektu, kurā iesaistīta sejas atpazīšanas tehnoloģija. Tajā sniegta plašāka informācija par organizatoriskiem un tehniskiem pasākumiem, kas jāņem vērā projekta ieviešanas laikā, un to nevajadzētu uzskatīt par izsmeļošu veicamo soļu/pasākumu sarakstu. Tas būtu jāaplūko arī saistībā ar EDAK Vadlīnijām 3/2019 par personas datu apstrādi, izmantojot videoierīces,[69] un jebkuru ES/EEZ regulu un EDAK vadlīnijām attiecībā uz mākslīgā intelekta izmantošanu.

Šajā pielikumā ir sniegtas pamatnostādnes, pamatojoties uz pieņēmumu, ka tiesībaizsardzības iestādes iegādāsies sejas atpazīšanas tehnoloģiju (kā standarta produktu). Ja tiesībaizsardzības iestāde plāno izstrādāt (turpināt apmācīt) sejas atpazīšanas tehnoloģiju, tad ir piemērojamas papildu prasības, lai izvēlētos nepieciešamās mācību, validācijas un testēšanas datu kopas, kas jāizmanto izstrādes laikā, un izstrādes vides lomas/pasākumus. Tāpat standarta produkts var prasīt papildu pielāgojumus paredzētajam lietojumam, un tādā gadījumā būtu jāizpilda iepriekš minētās prasības attiecībā uz testēšanas, validēšanas un apmācības datu kopu atlasi.

Piederība tai pašai tiesībaizsardzības iestādei pati par sevi nenodrošina pilnīgu piekļuvi biometriskajiem datiem. Tāpat kā jebkuras citas personas datu kategorijas, biometriskos datus, kas savākti konkrētam tiesībaizsardzības nolūkam saskaņā ar konkrētu juridisko pamatu, nevar izmantot bez pienācīga juridiskā pamata citam tiesībaizsardzības nolūkam (Direktīvas (ES) 2016/680 (Tiesībaizsardzības direktīva) 4. panta 2. punkts). Arī sejas atpazīšanas tehnoloģijas rīka izstrāde/apmācība tiek uzskatīta par atšķirīgu nolūku, un būtu jāizvērtē, vai biometrisko datu apstrāde, lai novērtētu veiktspēju/apmācītu tehnoloģiju, lai izvairītos no ietekmes uz datu subjektiem zemas veiktspējas dēļ, ir nepieciešama un samērīga, ņemot vērā apstrādes sākotnējo nolūku.

1. LOMAS UN PIENĀKUMI

Ja tiesībaizsardzības iestāde izmanto sejas atpazīšanas tehnoloģiju, lai veiktu savus uzdevumus, uz kuriem attiecas Tiesībaizsardzības direktīvas darbības joma (noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai krimināltvajāšana u. c. saskaņā ar Tiesībaizsardzības direktīvas 3. pantu), to var uzskatīt par sejas atpazīšanas tehnoloģijas datu pārzini. Tomēr tiesībaizsardzības iestādes sastāv no vairākām vienībām/nodaļām, kas var būt iesaistītas šajā apstrādē, vai nu nosakot sejas atpazīšanas tehnoloģijas pieteikuma procesu, vai arī to piemērojot praksē. Ņemot vērā šīs tehnoloģijas specifiku, var būt nepieciešams iesaistīt dažādas struktūrvienības, lai vai nu atbalstītu tās veiktspējas mērījumus, vai arī turpinātu tās apmācību.

Projektā, kurā iesaistīta sejas atpazīšanas tehnoloģija, tiesībaizsardzības iestādes[70] ietvaros var būt jāiesaista vairākas ieinteresētās personas:

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

[70] Turpmāk norādītās lomas raksturo dažādās ieinteresētās personas un to pienākumus sejas atpazīšanas tehnoloģijas projektā. Lai gan valoda, ko izmanto, lai aprakstītu šajā pielikumā minētās lomas, nav pārliecinoša, katrai tiesībaizsardzības iestādei ir jādefinē un jāpiešķir līdzīgas lomas atbilstoši savai organizācijai. Var gadīties,

- Augstākā līmeņa vadība — apstiprināt projektu pēc risku un iespējamo ieguvumu līdzsvarošanas.
- Datu aizsardzības speciālists un/vai tiesībaizsardzības iestādes juridiskais departaments — lai palīdzētu novērtēt konkrēta sejas atpazīšanas tehnoloģijas projekta īstenošanas likumību; lai palīdzētu veikt Novērtējumu par ietekmi uz datu aizsardzību; lai nodrošinātu datu subjektu tiesību ievērošanu un īstenošanu.
- Procesa īpašnieks — darbojas kā īpaša struktūrvienība kompetentajā tiesībaizsardzības iestādē, kas izstrādā projektu, lemj par sejas atpazīšanas tehnoloģijas projekta detaļām, tostarp par sistēmas veiktspējas prasībām; lemj par piemērotu taisnīguma metriku; nosaka ticamības rādītāju[71]; nosaka pieļaujamās novirzes robežvērtības; identificē iespējamos riskus, ko sejas atpazīšanas tehnoloģijas projekts rada attiecībā uz personu tiesībām un brīvībām (konsultējoties arī ar datu aizsardzības speciālistu un IT MI un/vai datu zinātnes departamentu (skat. zemāk), un iepazīstina ar tiem augstāko vadību. Pirms lēmuma pieņemšanas par sejas atpazīšanas tehnoloģijas projekta detaļām procesa īpašnieks konsultēsies arī ar atsauces datubāzes pārvaldnieku, lai izprastu gan atsauces datubāzes izmantošanas mērķi, gan arī tās tehniskās detaļas. Ja notiek iepirktās sejas atpazīšanas tehnoloģijas atkārtota apmācība, procesa īpašnieks būs atbildīgs arī par apmācības datu kopas atlasi. Tā kā procesa īpašnieks ir struktūrvienība, kuras uzdevums ir izstrādāt un lemt par projekta detaļām, viņš ir atbildīgs par Novērtējuma par ietekmi uz datu aizsardzību veikšanu.
- IT MI un/vai Datu zinātnes departaments — lai palīdzētu veikt Novērtējumu par ietekmi uz datu aizsardzību; lai izskaidrotu pieejamās metrikas sistēmas veiktspējas, godīguma[72] un iespējamās neobjektivitātes mērīšanai; lai ieviestu tehnoloģiju un tehniskos drošības pasākumus, lai novērstu nesankcionētu piekļuvi apkopotajiem datiem, kiberuzbrukumus utt. Iepirktās sejas atpazīšanas tehnoloģijas pārmācīšanas gadījumā IT MI vai Datu zinātnes nodaļa apmācīs sistēmu, pamatojoties uz procesa īpašnieka sniegto mācību datu kopu. Šis departaments būs atbildīgs arī par pasākumu noteikšanu, lai mazinātu risku, ko kopīgi identificējuši procesu īpašnieki (piemēram, mākslīgā intelekta specifiskos riskus, piemēram, uzbrukumus modeļa secinājumu veikšanai).
- Galalietotāji (piemēram, policijas darbinieki uz vietas vai kriminālistikas laboratorijās) — lai veiktu salīdzinājumu pret datubāzi, kritiski pārskatītu rezultātus, ņemot vērā iepriekšējos pierādījumus, un sniegtu atsauksmes procesa īpašniekam par nepatiesiem pozitīviem rezultātiem un norādēm par iespējamu diskrimināciju.
- Atsauces datubāzes vadītājs — īpašā vienība kompetentajā tiesībaizsardzības iestādē, kas atbild par atsauces datubāzes uzkrāšanu un pārvaldību, proti, datubāze, ar kuru tiks salīdzināti attēli, tostarp sejas attēlu dzēšana pēc noteiktā glabāšanas perioda. Šādu datubāzi var izveidot īpaši paredzētajam sejas atpazīšanas tehnoloģijas projektam vai arī tā var pastāvēt jau iepriekš, lai to varētu izmantot saderīgiem mērķiem. Atsauces datubāzes vadītāja pienākums ir noteikt, kad un kādos apstākļos sejas attēlus var glabāt, kā arī noteikt to datu saglabāšanas prasības (saskaņā ar laika vai citiem kritērijiem).

Tā kā lielākā daļa sejas atpazīšanas tehnoloģijas ieviešanas un izmantošanas gadījumu satur būtisku, augstu risku datu subjektu tiesībām un brīvībām, datu aizsardzības uzraudzības iestādei arī jābūt iesaistītai iepriekšējas apspriešanās kontekstā, kā noteikts Tiesībaizsardzības direktīvas 28. pantā.

ka vienība apvieno vairāk nekā vienu lomu, piemēram, procesa īpašnieks un atsauces datubāzes pārvaldnieks vai procesa īpašnieks un IT mākslīgā intelekta un/vai datu zinātnes nodaļa (ja procesa īpašnieka vienībai ir visas nepieciešamās tehniskās zināšanas).

[71] Uzticamības rādītājs ir prognozes (atbilstības) ticamības līmenis varbūtības formā. Piemēram, salīdzinot divas veidnes, ir 90 % ticamība, ka tās pieder vienai un tai pašai personai. Uzticamības rādītājs atšķiras no sejas atpazīšanas tehnoloģijas veiktspējas, tomēr tas ietekmē veiktspēju. Jo augstāks ticamības slieksnis, jo mazāk kļūdaini pozitīvu rezultātu un vairāk viltus negatīvu rezultātu sejas atpazīšanas tehnoloģijas rezultātos.

[72] Taisnīgumu var definēt kā negodīgas, nelikumīgas diskriminācijas, piemēram, dzimuma vai rases aizspriedumu, trūkumu.

2. SĀKUMS/PIRMS SEJAS ATPAZĪŠANAS TEHNOLOĢIJAS SISTĒMAS IEPIRKUMA

Procesa īpašniekam tiesībaizsardzības iestādē vispirms ir jābūt skaidrai izpratnei par procesu(-iem), kurā(-os) paredzēts izmantot sejas atpazīšanas tehnoloģiju (izmantošanas gadījums(-i)), un jānodrošina, ka ir juridisks pamats paredzētajam izmantošanas gadījumam. Pamatojoties uz to, viņiem ir nepieciešams:

- formāli aprakstīt lietošanas gadījumu. Jāapraksta risināmā problēma un veids, kā sejas atpazīšanas tehnoloģija nodrošinās risinājumu, kā arī jāizveido pārskats par procesu (uzdevumu), kurā tas tiks piemērots. Šajā sakarā tiesībaizsardzības iestādēm būtu jādokumentē vismaz[73]:
  - Procesā reģistrēto personas datu kategorijas
  - mērķi un konkrēti nolūki, kādiem sejas atpazīšanas tehnoloģija tiks izmantota, tostarp iespējamās sekas, kas datu subjektam var rasties pēc atbilstības.
  - Kad un kā tiks ievākti sejas attēli (tostarp informācija par šīs vākšanas kontekstu, piemēram, pie lidostas vārtiem, video no drošības kamerām ārpus noliktavas, kurā izdarīts noziegums utt., un datu subjektu kategorijas, kuru biometriskie dati tiks apstrādāti).
  - Datubāze, ar kuru attēli tiks salīdzināti (atsauces datubāze), kā arī informācija par to, kā tā tika izveidota, tās lielumu un tajā ietverto biometrisko datu kvalitāti.
  - Tiesībaizsardzības iestādes dalībnieki, kuri būs pilnvaroti izmantot sejas atpazīšanas tehnoloģijas sistēmu un rīkoties saistībā ar to tiesībaizsardzības kontekstā (to profili un piekļuves tiesības ir jānosaka procesa īpašniekam).
  - Paredzētais ievades datu glabāšanas periods vai brīdis, kas noteiks šā perioda beigas (piemēram, kriminālprocesa slēgšana vai izbeigšana saskaņā ar valsts procesuālajiem tiesību aktiem, attiecībā uz kuru tie sākotnēji tika vākti), kā arī jebkādas turpmākas darbības (šo datu dzēšana, anonimizācija un izmantošana statistikas vai pētniecības nolūkos utt.).
  - Reģistrācijas ieviešana un reģistrēto žurnālu un ierakstu pieejamība.
  - Veiktspējas rādītāji (piemēram, precizitāte, precizitāte, atsaukšana, F1 rādītājs) un to minimālās pieļaujamās robežvērtības.[74]
  - Aplēses par to, cik daudz cilvēku tiks pakļauti sejas atpazīšanas tehnoloģijai, kurā laikposmā/gadījumā.
- Veikt nepieciešamības un proporcionalitātes novērtējumu[75]. Fakts, ka šī tehnoloģija eksistē, nedrīkstētu būt virzītājspēks, lai to izmantotu. Procesa īpašniekam vispirms jānovērtē, vai paredzētajai apstrādei ir atbilstošs juridiskais pamats. Šajā nolūkā ir jākonsultējas ar datu aizsardzības speciālistu un juridisko dienestu. Sejas atpazīšanas tehnoloģijas ieviešanas virzītājspēkam vajadzētu būt tam, ka tas ir nepieciešams un samērīgs risinājums konkrēti definētai

[73] I pielikumā ir sniegts to elementu saraksts, kas palīdz kontrolierim aprakstīt sejas atpazīšanas tehnoloģijas lietojuma gadījumu.

[74] Lai novērtētu sejas atpazīšanas tehnoloģijas sistēmas darbību, ir dažādi rādītāji. Katra metrika sniedz atšķirīgu priekšstatu par sistēmas rezultātiem, un tās spēja sniegt adekvātu priekšstatu par to, vai sejas atpazīšanas tehnoloģijas sistēma darbojas labi, ir atkarīga no sejas atpazīšanas tehnoloģijas izmantošanas gadījuma. Ja uzsvars tiek likts uz to, lai sasniegtu augstus procentus attiecībā uz pareizu sejas sakritību, var izmantot tādus rādītājus kā precizitāte un atsaukšana. Tomēr šie rādītāji nemēra, cik labi sejas atpazīšanas tehnoloģija apstrādā negatīvus piemērus (cik daudzus no tiem sistēma ir nepareizi saskaņojusi). Procesa īpašniekam ar IT MI un datu zinātnes nodaļas atbalstu ir jāspēj noteikt veiktspējas prasības un izteikt tās ar vispiemērotāko metriku atbilstoši sejas atpazīšanas tehnoloģijas lietojuma gadījumam.

[75] Var apsvērt turpmākus pasākumus nepieciešamības gadījumā attiecībā uz sistēmas pielāgošanu un izmantošanu, tāpēc nepieciešamības un samērīguma novērtējuma laikā lietošanas gadījuma aprakstu var nedaudz mainīt.

tiesībaizsardzības iestādes problēmai. Tas ir jānovērtē atkarībā no nozieguma mērķa/nopietnības/to personu skaita, kuras nav iesaistītas, bet kuras ietekmē sejas atpazīšanas tehnoloģijas sistēma. Lai novērtētu likumību, būtu jāņem vērā vismaz šādi aspekti: DAT[76], VDAR[77] [78], jebkāds spēkā esošs tiesiskais regulējums attiecībā uz MI[79] un visas pievienotās pamatnostādnes, ko sniegušas datu aizsardzības uzraudzības iestādes (piemēram, EDAK pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces[80]). Šie ES tiesību akti vienmēr būtu jāsaskaņo ar piemērojamām valsts prasībām, jo īpaši krimināltiesību procesuālo tiesību jomā. Proporcionalitātes novērtējumā būtu jānosaka datu subjektu pamattiesības, kuras var tikt skartas (papildus privātuma un datu aizsardzības tiesībām). Tajā arī jāapraksta un jāņem vērā visi ierobežojumi (vai ierobežojumu neesamība), kas lietošanas gadījumā noteikti sejas atpazīšanas tehnoloģijas sistēmai. Piemēram, vai sistēma darbosies pastāvīgi vai uz laiku un vai tā būs ierobežota līdz ģeogrāfiskai teritorijai.

- Veikt Novērtējumu par ietekmi uz datu aizsardzību[81]. Novērtējums par ietekmi uz datu aizsardzību būtu jāveic, jo sejas atpazīšanas tehnoloģijas ieviešana tiesībaizsardzības jomā var radīt augstu risku personu tiesībām un brīvībām[82]. Novērtējumā par ietekmi uz datu aizsardzību jo īpaši būtu jāietver: paredzamo apstrādes darbību vispārīgs apraksts[83], datu subjektu tiesību un brīvību apdraudējumu novērtējums[84], pasākumi, kas paredzēti, lai novērstu šos apdraudējumus, aizsardzības pasākumi, drošības pasākumi un mehānismi, lai nodrošinātu personas datu aizsardzību un pierādītu atbilstību. Novērtējums par ietekmi uz datu aizsardzību ir nepārtraukts process, tāpēc būtu jāpievieno jauni apstrādes elementi un būtu jāatjaunina riska novērtējums katrā projekta posmā.
- Iegūt apstiprinājumu no augstākās vadības, izskaidrojot riskus datu subjektu tiesībām un brīvībām (no izmantošanas gadījuma un tehnoloģijas) un attiecīgos riska pārvaldības plānus.

[76] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināls odus, un par šādu datu brīvu apriti.

[77] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

[78] Gadījumos, kad zinātniskam projektam, kura mērķis ir izpētīt sejas atpazīšanas tehnoloģijas izmantošanu, būtu jāapstrādā personas dati, taču uz šādu apstrādi neattiecas Tiesībaizsardzības direktīvas 4. panta 3. punkts, parasti būtu piemērojama VDAR (Tiesībaizsardzības direktīvas 9. panta 2. punkts). Tādu izmēģinājuma projektu gadījumā, kuriem sekotu tiesībaizsardzības pasākumi, joprojām būtu piemērojama Tiesībaizsardzības direktīva.

[79] Piemēram, ir iesniegts priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULAI, AR KO NOSAKA SASKAŅOTUS NOTEIKUMUS PAR MĀKSLĪGO INTELEKTU (MĀKSLĪGĀ INTELEKTA AKTS) un groza dažus Savienības tiesību aktus, tomēr tas vēl nav pieņemts kā regula.

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

[81] Papildu norādījumi par Novērtējumu par ietekmi uz datu aizsardzību ir atrodami šeit: Pamatnostādnes Novērtējumu par ietekmi uz datu aizsardzību un noteikšanu, vai apstrāde "var radīt augstu risku" Regulas 2016/679 nolūkos, WP 248 red. 01, pieejamas tīmekļvietnē: https://ec.europa.eu/newsroom/article29/items/611236 un EDAU instrumentu kopums "Atbildība uz vietas", II daļa, pieejama tīmekļvietnē: https://edps.europa.eu/node/4582_en

[82] Sejas atpazīšanas tehnoloģija atkarībā no izmantošanas gadījuma var ietilpt šādos kritērijos, kas izraisa augsta riska apstrādi (saskaņā ar Pamatnostādnēm par novērtējumu par ietekmi uz datu aizsardzību, WP 248 red. 01): Sistemātiska uzraudzība, liela mēroga apstrādāti dati, datu kopu salīdzināšana vai kombinēšana, inovatīva izmantošana vai jaunu tehnoloģisko vai organizatorisko risinājumu piemērošana.

[83] Apstrādes apraksts, kā arī nepieciešamības un samērīguma novērtējums, kā jau aprakstīts iepriekš minētajos posmos, papildus riska novērtējumam ir arī daļa no Novērtējuma par ietekmi uz datu aizsardzību. Vajadzības gadījumā Novērtējums par ietekmi uz datu aizsardzību tiks sniegts detalizētāks personas datu plūsmu apraksts.

[84] Datu subjektiem radīto risku analīzei būtu jāietver riski, kas saistīti ar salīdzināmo sejas attēlu atrašanās vietu (lokāli/attālināti), riski, kas saistīti ar apstrādātājiem/apakšapstrādātājiem, kā arī riski, kas raksturīgi mašīnmācībai, kad tā tiek izmantota (piemēram, datu saindēšana, pretēju piemēru izmantošana).

3. IEPIRKUMA LAIKĀ UN PIRMS SEJAS ATPAZĪŠANAS TEHNOLOĢIJAS IEVIEŠANAS

- Izlemt kritērijus sejas atpazīšanas tehnoloģijas (algoritma) izvēlei. Procesa īpašniekam ar IT MI un/vai datu zinātnes departamenta palīdzību būtu jālemj par algoritma izvēles kritērijiem. Praksē tie ietvertu godīgumu un veiktspējas rādītājus, par kuriem lemts lietošanas gadījuma aprakstā. Šādos kritērijos jāiekļauj arī informācija par datiem, ar kuriem algoritms tika apmācīts. Apmācības, testēšanas un validēšanas komplektā ir pietiekami jāiekļauj visu to datu subjektu raksturlielumu paraugi, uz kuriem jāattiecina sejas atpazīšanas tehnoloģija (jāņem vērā, piemēram, vecums, dzimums un rase), lai mazinātu neobjektivitāti. Sejas atpazīšanas tehnoloģijas pakalpojumu sniedzējam jāsniedz informācija un metrikas par sejas atpazīšanas tehnoloģijas apmācību, testēšanas un validācijas datu kopām un jāapraksta pasākumi, kas veikti, lai novērtētu un mazinātu iespējamo nelikumīgo diskrimināciju un neobjektivitāti. Procesa īpašniekam, ja iespējams, ir jāpārbauda, vai pakalpojumu sniedzējam bija juridisks pamats izmantot šo datu kopu algoritmu apmācībai (pamatojoties uz informāciju, ko pakalpojumu sniedzējs darīs pieejamu). Turklāt procesa īpašniekam būtu jānodrošina, ka sejas atpazīšanas tehnoloģijas pakalpojumu sniedzējs piemēro ar biometriskajiem datiem saistītus drošības standartus, piemēram, ISO/IEC 24745, kas sniedz norādījumus par biometriskās informācijas aizsardzību saskaņā ar dažādām prasībām attiecībā uz konfidencialitāti, integritāti un atjaunojamību/atsaucamību glabāšanas un nosūtīšanas laikā, un prasībām un pamatnostādnēm attiecībā uz drošu un privātumam atbilstošu biometriskās informācijas pārvaldību un apstrādi.

- Pārmācīt algoritmu (ja nepieciešams). Procesa īpašniekam būtu jānodrošina, ka sejas atpazīšanas tehnoloģijas sistēmas precizēšana, lai panāktu lielāku precizitāti pirms tās izmantošanas, arī ir daļa no iepirktajiem pakalpojumiem. Ja ir nepieciešama papildu apmācība par iegūto sejas atpazīšanas tehnoloģijas sistēmu, lai nodrošinātu precizitātes rādītājus, procesa īpašniekam, izņemot lēmuma par pārmācīšanu pieņemšanu, ar IT MI un/vai datu zinātnes departamenta palīdzību ir jālemj par atbilstošu, reprezentatīvu datu kopumu, kas jāizmanto, un jāpārbauda datu izmantošanas likumīgums.
- Noteikt atbilstošus aizsardzības pasākumus, lai novērstu riskus, kas saistīti ar drošību, neobjektivitāti un zemu sniegumu. Tas ietver arī procesa izveidi, lai uzraudzītu sejas atpazīšanas tehnoloģiju pēc tās izmantošanas (reģistrēšana un atgriezeniskā saite, lai nodrošinātu rezultātu precizitāti un taisnīgumu). Turklāt nodrošināt, ka tiek identificēti, mērīti un mazināti riski, kas raksturīgi dažām mašīnmācīšanās un sejas atpazīšanas tehnoloģijas sistēmām (piemēram, saindēšanās ar datiem, pretrunīgi piemēri, modeļu inversija, baltās kastes secinājumi). Procesa īpašniekam jānosaka arī atbilstoši drošības pasākumi, lai nodrošinātu, ka tiks ievērotas pārkvalifikācijas datu kopā iekļauto biometrisko datu saglabāšanas prasības.
- Sejas atpazīšanas tehnoloģijas sistēmas dokumentēšana. Tajā būtu jāiekļauj sejas atpazīšanas tehnoloģijas sistēmas vispārīgs apraksts, detalizēts sejas atpazīšanas tehnoloģijas sistēmas elementu un tās izveides procesa apraksts, detalizēta informācija par sejas atpazīšanas tehnoloģijas sistēmas uzraudzību, darbību un kontroli, kā arī detalizēts tās risku un to mazināšanas pasākumu apraksts. Šajā dokumentācijā iekļautie elementi ietvers galvenos sejas atpazīšanas tehnoloģijas sistēmas apraksta elementus no iepriekšējiem posmiem (skat. iepriekš), tomēr tie tiks papildināti ar informāciju, kas saistīta ar sistēmas darbības uzraudzību un izmaiņu piemērošanu, tostarp jebkādiem versiju atjauninājumiem un/vai atkārtotu apmācību.
- Izveidot lietotāja rokasgrāmatas, kurās izskaidrota tehnoloģija un lietošanas gadījumi. Tajos skaidri jāizskaidro visi scenāriji un priekšnosacījumi, saskaņā ar kuriem sejas atpazīšanas tehnoloģija tiks izmantota.

- Apmācīt galalietotājus, kā izmantot tehnoloģiju. Šādās apmācībās ir jāizskaidro tehnoloģijas iespējas un ierobežojumi, lai lietotāji varētu saprast, kādos apstākļos tā ir jāpiemēro un kādos gadījumos tā var būt neprecīza. Šādas apmācības arī palīdzēs mazināt riskus, kas saistīti ar algoritma iznākuma nepārbaudi/kritizēšanu.
- Apspriesties ar datu aizsardzības uzraudzības iestādi saskaņā ar Tiesībaizsardzības direktīvas 28. panta 1. punkta b) apakšpunktu. Sniegt informāciju saskaņā ar Tiesībaizsardzības direktīvas 13. pantu, lai informētu datu subjektus par apstrādi un viņu tiesībām. Šajos paziņojumos ir jāvēršas pie datu subjektiem piemērotā valodā, lai viņi varētu saprast apstrādi un izskaidrot tehnoloģijas pamatelementus, tostarp precizitātes rādītājus, mācību datu kopas un pasākumus, kas veikti, lai novērstu diskrimināciju un algoritma zemo precizitāti.

4. IETEIKUMI PĒC SEJAS ATPAZĪŠANAS TEHNOLOĢIJAS IEVIEŠANAS

- Nodrošināt cilvēka iejaukšanos un rezultātu pārraudzību. Nekad neveiciet nekādus pasākumus attiecībā uz personu, pamatojoties tikai uz sejas atpazīšanas tehnoloģijas rezultātiem (tas nozīmētu, ka tiek pārkāpts Tiesībaizsardzības direktīvas 11. pants — automatizēta individuālu lēmumu pieņemšana, kam ir juridiskas vai citas līdzīgas sekas attiecībā uz datu subjektu). Nodrošināt, ka tiesībaizsardzības iestādes amatpersona pārskata sejas atpazīšanas tehnoloģijas rezultātus. Nodrošināt arī to, ka tiesībaizsardzības iestādes lietotāji izvairās no automatizācijas neobjektivitātes, izmeklējot pretrunīgu informāciju un kritiski apstrīdot tehnoloģijas rezultātus. Šajā nolūkā ir svarīga pastāvīga apmācība un informētības palielināšana galalietotājiem, tomēr augstākajai vadībai būtu jānodrošina pietiekami cilvēkresursi, lai veiktu efektīvu pārraudzību. Tas nozīmē, ka katram aģentam ir jānodrošina pietiekami daudz laika, lai kritiski pārbaudītu tehnoloģijas rezultātus. Reģistrēt, izmērīt un novērtēt, cik lielā mērā cilvēka veiktā uzraudzība maina sejas atpazīšanas tehnoloģijas sākotnējo lēmumu.
- Uzraudzīt un novērst sejas atpazīšanas tehnoloģijas modeļa novirzi (veiktspējas pasliktināšanos), kad modelis ir ieviests ražošanā.
- Izveidot procesu, lai regulāri un ikreiz, kad mainās tehnoloģija vai lietošanas gadījums, atkārtoti novērtētu riskus un drošības pasākumus.
- Dokumentēt jebkuras izmaiņas sistēmā visā tās dzīves ciklā (piemēram, atjauninājumi, atkārtota apmācība).
- Izveidot procesu, kā arī ar to saistītās tehniskās iespējas, lai izskatītu datu subjektu piekļuves pieprasījumus. Tehniskajām iespējām datu ieguvei, ja rodas nepieciešamība tos sniegt datu subjektiem, ir jābūt gatavām, pirms tiek iesniegts jebkurš pieprasījums.
- Nodrošināt, ka ir ieviestas procedūras datu aizsardzības pārkāpumu gadījumos. Ja notiek personas datu aizsardzības pārkāpums, kas ietver biometriskos datus, riski, visticamāk, būs augsti. Šādā gadījumā visiem iesaistītajiem lietotājiem vajadzētu būt informētiem par attiecīgajām procedūrām, kas jāievēro, būtu nekavējoties jāinformē datu aizsardzības speciālistu un datu subjektus.

III PIELIKUMS. PRAKTISKI PIEMĒRI

Pastāv daudz dažādu praktisku sejas atpazīšanas izmantošanas iespēju un nolūku, piemēram, kontrolētā vidē, piemēram, robežšķērsošanas vietās, kontrolpārbaudēs ar datiem no policijas datubāzēm vai personas datiem, kurus datu subjekts ir acīmredzami publiskojis, tiešraides kameru ierakstos (sejas atpazīšana tiešraidē) u. c. Rezultātā personas datu un citu pamattiesību un pamatbrīvību aizsardzības riski dažādos izmantošanas gadījumos ievērojami atšķiras. Lai atvieglotu nepieciešamības un proporcionalitātes novērtēšanu, kas būtu jāveic pirms lēmuma pieņemšanas par sejas atpazīšanas iespējamo ieviešanu, pašreizējās pamatnostādnēs ir sniegts neizsmeļošs saraksts ar sejas atpazīšanas tehnoloģijas iespējamiem lietojumiem tiesībaizsardzības jomā.

Izklāstītie un novērtētie scenāriji ir balstīti uz **hipotētiskām** situācijām, un to mērķis ir ilustrēt dažus konkrētus sejas atpazīšanas tehnoloģijas izmantošanas veidus un sniegt palīdzību katra atsevišķā gadījumā, kā arī noteikt vispārēju satvaru. Tie necenšas būt izsmeļoši un neskar notiekošas vai turpmākas procedūras, ko valsts uzraudzības iestāde veic attiecībā uz sejas atpazīšanas tehnoloģiju izstrādi, eksperimentēšanu vai īstenošanu. Šo scenāriju izklāstam būtu jākalpo tikai tam, lai uzskatāmi parādītu šajā dokumentā jau sniegtās vadlīnijas politikas veidotājiem, likumdevējiem un tiesībaizsardzības iestādēm, kad tās plāno un paredz sejas atpazīšanas tehnoloģiju ieviešanu, lai nodrošinātu pilnīgu atbilstību ES tiesību aktu kopumam personas datu aizsardzības jomā. Šajā kontekstā jāatceras, ka pat līdzīgās sejas atpazīšanas tehnoloģijas izmantošanas situācijās atsevišķu elementu esamība vai neesamība var novest pie atšķirīga nepieciešamības un samērīguma novērtējuma iznākuma.

1 1. SCENĀRIJS

1.1. Apraksts

Automatizēta robežkontroles sistēma, kas ļauj automātiski šķērsot robežu, autentificējot ES pilsoņu un citu ceļotāju, kuri šķērso robežu, elektroniskajā ceļošanas dokumentā glabāto biometrisko attēlu un konstatējot, ka pasažieris ir dokumenta likumīgais īpašnieks.

Šāda verifikācija/autentifikācija ietver tikai individuālu sejas atpazīšanu un tiek veikta kontrolētā vidē (piemēram, lidostas e-vārtos). Robežšķērsošanas punktu šķērsojošā ceļotāja biometriskie dati tiek uztverti, kad viņš tiek skaidri aicināts paskatīties uz e-vārtos esošo kameru, un tiek salīdzināti ar uzrādītā dokumenta (pases, personas apliecības u. c.), kas tiek izsniegts saskaņā ar īpašām tehniskām prasībām, datiem.

Tajā pašā laikā, lai gan apstrāde šādos gadījumos principā neietilpst Tiesībaizsardzības direktīvas darbības jomā, pārbaudes iznākumu var izmantot arī personas datu (burtciparu) salīdzināšanai ar tiesībaizsardzības datubāzēm robežkontroles ietvaros, un tādējādi tā var ietvert darbības ar būtisku juridisku ietekmi uz datu subjektu, piemēram, apcietināšanu saskaņā ar brīdinājumu Šengenas Informācijas sistēmā. Noteiktos apstākļos biometriskos datus var izmantot arī, lai meklētu sakritības tiesībaizsardzības iestāžu datubāzēs (šādā gadījumā šajā posmā tiktu veikta identifikācijas "viens pret daudziem").

Biometriskā attēla apstrādes rezultātam ir tieša ietekme uz datu subjektu: tikai veiksmīgas verifikācijas gadījumā tas ļauj šķērsot robežu. Neveiksmīgas identifikācijas gadījumā robežsargiem jāveic otrā pārbaude, lai pārliecinātos, ka datu subjekts atšķiras no identifikācijas dokumentā norādītā.

Ja tiek identificēts Šengenas Informācijas sistēmas vai valsts brīdinājums, robežsargiem jāveic atkārtota pārbaude un nepieciešamās papildu pārbaudes, un pēc tam jāveic nepieciešamās darbības, piemēram, persona jāaiztur, jāinformē attiecīgās iestādes.

Informācijas avots: • Datu subjektu veidi: ☒ visas personas, kas šķērso robežas • Attēla avots: ☒ cits (ID dokuments) • Saistība ar noziegumu: ☒ nav nepieciešams • Informācijas iegūšanas veids: ☒ kabīnē vai kontrolētā vidē • Konteksts — ietekme uz citām pamattiesībām: Jā, proti, ☒ tiesības uz brīvu pārvietošanos ☒ tiesības uz patvērumu Atsauces datubāze (ar kuru salīdzina iegūto informāciju): • Specifiskums: ☒ īpašas datubāzes, kas saistītas ar robežkontroli Algoritms: • Pārbaudes veids: ☒ pārbaude "viens pret vienu" (autentifikācija). Rezultāti: • Ietekme ☒ tieša (datu subjektam ir atļauta vai aizliegta iebraukšana) • Automatizēts lēmums: ☒ Jā

1.2. Piemērojamais tiesiskais regulējums

Kopš 2004. gada saskaņā ar Padomes Regulu (EK) Nr. 2252/2004[85] dalībvalstu izdotās pasēs un citos ceļošanas dokumentos ir jābūt biometriskam sejas attēlam, kas saglabāts dokumentā iekļautā elektroniskajā mikroshēmā.

Šengenas Robežu kodeksā[86] ir noteiktas prasības attiecībā uz personu robežpārbaudēm pie ārējās robežas. ES pilsoņiem un citām personām, kuras izmanto tiesības brīvi pārvietoties saskaņā ar Savienības tiesību aktiem, minimālajās pārbaudēs būtu jāietver viņu ceļošanas dokumentu pārbaude, attiecīgā gadījumā izmantojot tehniskas ierīces. Pēc tam Šengenas Robežu kodekss ir grozīts ar Regulu (ES) 2017/2225[87], ar ko cita starpā ir ieviestas "e-vārtu", "automatizētas robežkontroles sistēmas" un "pašapkalpošanās sistēmas" definīcijas, kā arī iespēja apstrādāt biometriskos datus robežpārbaužu veikšanai.

Tādējādi var pieņemt, ka pastāv skaidrs un paredzams juridiskais pamats, kas atļauj šāda veida personas datu apstrādi. Turklāt tiesiskais regulējums ir pieņemts Savienības līmenī un ir tieši piemērojams dalībvalstīm.

1.3. Nepieciešamība un samērīgums — nozieguma mērķis/smagums

ES pilsoņu identitātes pārbaude automatizētā robežkontroles sistēmā, izmantojot viņu biometrisko attēlu, ir viens no robežkontroles elementiem pie ES ārējās robežas. Tādējādi tā ir tieši saistīta ar robežu drošību un kalpo Savienības atzītam vispārējas nozīmes mērķim. Turklāt ABC vārti palīdz paātrināt pasažieru apkalpošanu un mazināt cilvēka kļūdu risku. Turklāt šajā scenārijā iejaukšanās apjoms, pakāpe un intensitāte ir daudz ierobežotāka salīdzinājumā ar citiem sejas atpazīšanas veidiem. Tomēr

[85] PADOMES REGULA (EK) Nr. 2252/2004 (2004. gada 13. decembris) par drošības elementu un biometrijas standartiem dalībvalstu izdotās pasēs un ceļošanas dokumentos.
[86] EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/399 (2016. gada 9. marts) par Savienības Kodeksu par noteikumiem, kas reglamentē personu pārvietošanos pār robežām (Šengenas Robežu kodekss).
[87] Eiropas Parlamenta un Padomes Regula (ES) 2017/2225 (2017. gada 30. novembris), ar ko groza Regulu (ES) 2016/399 attiecībā uz ieceļošanas/izceļošanas sistēmas izmantošanu.

biometrisko datu apstrāde rada papildu riskus datu subjektiem, kas kompetentajai iestādei, kura izvērš un izmanto sejas atpazīšanas tehnoloģiju, ir pienācīgi jārisina un jāsamazina.

1.4. Secinājums

ES pilsoņu identitātes pārbaude saistībā ar automatizētu robežkontroli ir nepieciešams un samērīgs pasākums, kamēr vien ir ieviesti atbilstoši aizsardzības pasākumi, jo īpaši nolūka ierobežojuma, datu kvalitātes, pārredzamības un augsta drošības līmeņa principu piemērošana.

2 2. SCENĀRIJS

2.1. Apraksts

Bērnu nolaupīšanas upuru identifikācijas sistēmu nosaka tiesībaizsardzības iestādes. Pilnvarots policijas darbinieks var veikt aizdomās par nolaupīšanu turamā bērna biometrisko datu salīdzināšanu ar bērnu nolaupīšanas upuru datubāzi, ievērojot stingrus nosacījumus, vienīgi ar mērķi identificēt nepilngadīgos, kuri varētu atbilst pazudušā bērna aprakstam, par kuru ir uzsākta izmeklēšana un izdots brīdinājums.

Attiecīgā apstrāde būtu personas sejas vai attēla, kas varētu atbilst pazudušā bērna aprakstam, salīdzināšana ar datubāzē saglabātajiem attēliem. Šāda apstrāde notiktu konkrētos gadījumos, nevis sistemātiski.

Datubāze, kurai tiks piemērota salīdzināšana, tiek aizpildīta ar pazudušo bērnu attēliem, par kuriem ir ziņots par aizdomām par bērnu nolaupīšanu, apdraudējumu bērna dzīvībai vai fiziskajai neaizskaramībai un par kuriem ir sākta kriminālizmeklēšana tiesu iestādē, un par kuriem ir izdots brīdinājums par bērnu nolaupīšanu. Dati tiek ievākti saskaņā ar procedūrām, ko noteikusi kompetentā tiesībaizsardzības iestāde, proti, policijas darbinieki, kas ir pilnvaroti veikt tiesu policijas uzdevumus. Reģistrēto personas datu kategorijas ir šādas:

- identitāte, segvārds, pieņemts vārds, izcelsme, valstspiederība, adreses, e-pasta adreses, tālruņa numuri;
- dzimšanas datums un vieta;
- informācija par bioloģisko radniecību;
- fotogrāfija ar tehniskām īpašībām, kas ļauj izmantot sejas atpazīšanas ierīci, un citas fotogrāfijas.

Pilnvarotā amatpersona pārskata un pārbauda arī salīdzināšanas rezultātus, lai apstiprinātu iepriekšējos pierādījumus ar salīdzinājuma rezultātu un izslēgtu jebkādus iespējamos viltus pozitīvos rezultātus.

Bērnu attēlus un personas datus var glabāt tikai uz brīdinājuma laiku, un tie ir nekavējoties jāizdzēš pēc kriminālprocesa slēgšanas vai izbeigšanas saskaņā ar valsts procedūrām, kuru dēļ tie ir ievietoti datubāzē.

Lai gan biometrisko datu uzglabāšanas periods datubāzē var būt paredzēts salīdzinoši ilgs un noteikts saskaņā ar valsts tiesību aktiem, datu subjekta tiesību īstenošana un jo īpaši tiesības uz labošanu un izdzēšanu nodrošina papildu garantiju, lai ierobežotu iejaukšanos attiecīgo datu subjektu tiesībās uz personas datu aizsardzību.

Informācijas avots:

- Datu subjektu veidi: ☒ bērni
- Attēla avots ☒ cits: nav iepriekš noteikts, aizdomas par bērna nolaupīšanu
- Saistība ar noziegumu ☒ netieša laika ziņā ☒ netieša ģeogrāfiski
- Informācijas iegūšanas veids: ☒ kabīnē vai kontrolētā vidē
- Konteksts: ietekme uz citām pamattiesībām ☒ Jā, proti, ☒ dažādi

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums ☒ specifiska datubāze

Algoritms:

- Pārbaudes veids: ☒ pārbaude "viens pret daudziem"

Rezultāti:

- Ietekme ☒ tieša
- Automatizēts lēmums: ☒ NĒ, obligāta pārbaude, ko veic pilnvarota amatpersona

Juridiskā analīze:

- Piemērojamais tiesiskais regulējums: ☒ šai apstrādei specifiskie valsts tiesību akti (sejas atpazīšana)

2.2. Piemērojamais tiesiskais regulējums

Valsts tiesību aktos ir paredzēts īpašs tiesiskais regulējums, ar ko izveido datubāzi, nosakot apstrādes nolūkus, kā arī kritērijus datubāzes aizpildīšanai, piekļuvei un izmantošanai. Tās īstenošanai nepieciešamie likumdošanas pasākumi paredz arī glabāšanas perioda noteikšanu, kā arī atsauci uz piemērojamiem integritātes un konfidencialitātes principiem. Likumdošanas pasākumi paredz arī kārtību, kādā tiek sniegta informācija datu subjektam, un šajā gadījumā personai(-ām), kam ir vecāku atbildība, kā arī datu subjekta tiesību izmantošanai un iespējamiem ierobežojumiem, ja piemērojams. Sagatavojot priekšlikumu par attiecīgo tiesību aktu, bija jākonsultējas ar valsts uzraudzības iestādi.

2.3. Nepieciešamība un samērīgums — nozieguma nolūks/smagums/to personu skaits, kuras nav iesaistītas, bet kuras skar apstrāde

Apstrādes nosacījumi un aizsardzības pasākumi

Sejas atpazīšanas salīdzināšanu kā galējo līdzekli var veikt pilnvarota amatpersona tikai tad, ja nav pieejami citi mazāk traucējoši līdzekļi un ja tas ir absolūti nepieciešams, piemēram, ja ir šaubas par ceļojošā nepilngadīgā personu apliecinoša dokumenta autentiskumu un/vai pēc tam, kad ir pārskatīti iepriekšējie pierādījumi un savāktie materiāli, kas norāda uz iespējamu atbilstību pazuduša bērna aprakstam, par kuru tiek veikta kriminālizmeklēšana.

Papildu aizsardzības pasākumi tiek nodrošināti arī ar sejas atpazīšanas salīdzināšanas obligātu pārskatīšanu un pārbaudi, ko veic pilnvarota amatpersona, lai apstiprinātu iepriekšējos pierādījumus ar salīdzinājuma rezultātu un izslēgtu jebkādus iespējamus viltus pozitīvus rezultātus.

Izvirzītais mērķis

Datubāzes izveide kalpo svarīgiem vispārējo sabiedrības interešu mērķiem, jo īpaši noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai vai saukšanai pie atbildības par tiem vai kriminālsodu izpildei, kā arī citu personu tiesību un brīvību aizsardzībai. Datubāzes izveide un paredzētā apstrāde, šķiet, palīdz identificēt nolaupītos bērnus, un tāpēc to var uzskatīt par piemērotu pasākumu, lai atbalstītu leģitīmo mērķi izmeklēt šādus noziegumus un saukt pie atbildības par tiem.

Datu bāzes mērķis un datu kopas

Apstrādes nolūki ir skaidri definēti tiesību aktos, un datubāzi izmanto tikai, lai identificētu pazudušus bērnus, par kuriem ir radušās aizdomas par nolaupīšanu un ir uzsākta kriminālizmeklēšana tiesu iestādes uzraudzībā, un par kuriem ir izdots brīdinājums par bērna nolaupīšanu. Likumā paredzētie nosacījumi attiecībā uz datubāzes datu kopām ir vērsti uz to, lai stingri ierobežotu datubāzē iekļaujamo datu subjektu un personas datu skaitu. Persona, kam ir vecāku atbildība par bērnu, ir jāinformē par veikto apstrādi un bērna tiesību īstenošanas nosacījumiem attiecībā uz biometrisko apstrādi, kas paredzēta identifikācijas nolūkā, vai attiecībā uz datubāzē glabātajiem bērna personas datiem.

2.4. Secinājums

Ņemot vērā paredzētās apstrādes nepieciešamību un samērīgumu, kā arī bērna intereses, veicot šādu personas datu apstrādi, un ar nosacījumu, ka ir paredzētas pietiekamas garantijas, lai jo īpaši nodrošinātu datu subjekta tiesību īstenošanu, jo īpaši ņemot vērā to, ka tiks apstrādāti bērnu dati, šādu sejas atpazīšanas apstrādes piemērošanu var uzskatīt par iespējami saderīgu ar ES tiesībām.

Turklāt, ņemot vērā apstrādes veidu un izmantoto tehnoloģiju, kas ietver augstu risku attiecīgā datu subjekta tiesībām un brīvībām, EDAK uzskata, ka, sagatavojot priekšlikumu leģislatīvam pasākumam, kas jāpieņem valsts parlamentam, vai regulatīvam pasākumam, kura pamatā ir šāds likumdošanas pasākums, kas attiecas uz paredzēto apstrādi, ir jāietver iepriekšēja apspriešanās ar uzraudzības iestādi, lai nodrošinātu konsekvenci un atbilstību piemērojamajam tiesiskajam regulējumam, sal. Tiesībaizsardzības direktīvas 28.2. pants.

3 3. SCENĀRIJS

3.1. Apraksts

Policijas iejaukšanās laikā masu nekārtībās un pēc tam veiktajās izmeklēšanās vairākas personas ir identificētas kā aizdomās turamie, piemēram, iepriekšējās izmeklēšanās, izmantojot videonovērošanas kameru ierakstus vai lieciniekus. Šo aizdomās turamo personu attēli tiek salīdzināti ar to personu attēliem, kuras ir fiksētas videonovērošanas kamerās vai mobilajās ierīcēs nozieguma vietā vai apkārtējā teritorijā.

Lai iegūtu detalizētākus pierādījumus par personām, kuras tiek turētas aizdomās par piedalīšanos nemieros saistībā ar demonstrāciju, policija izveido datubāzi, kas sastāv no attēlu materiāliem, kuriem ir vāja vietējā un laika saistība ar nemieriem. Datubāze ietver privātus ierakstus, ko policijai augšupielādējuši pilsoņi, materiālus no sabiedriskā transporta videonovērošanas kamerām, policijas īpašumā esošus videonovērošanas materiālus un plašsaziņas līdzekļu publicētos materiālus bez konkrētiem ierobežojumiem vai aizsardzības pasākumiem. Smagas noziedzīgas rīcības atspoguļošana nav priekšnoteikums datņu ievākšanai datubāzē. Tāpēc datubāzē tiek saglabāti dati par personām, kas nav piedalījušās nekārtībās — ievērojamu daļu vietējo iedzīvotāju, kuri demonstrācijas brīdī nejauši gājuši garām vai piedalījušies demonstrācijā, bet ne nekārtībās. Tie ir tūkstošiem video un attēlu datņu.

Izmantojot sejas atpazīšanas programmatūru, visām šajās datnēs redzamajām sejām tiek piešķirts unikāls sejas ID. Pēc tam atsevišķu aizdomās turamo personu sejas tiek automātiski salīdzinātas ar šiem sejas identifikatoriem. Datubāze, kas sastāv no visiem biometrisko seju šabloniem tūkstošos video un attēlu datņu, tiek uzglabāta līdz brīdim, kad visas iespējamās izmeklēšanas tiek pabeigtas. Pozitīvas atbilsmes izskata atbildīgie darbinieki, kuri pēc tam pieņem lēmumu par turpmāku rīcību. Tas var ietvert datubāzē esošās datnes sasaistīšanu ar attiecīgās personas krimināllietu, kā arī papildu pasākumus, piemēram, minētās personas nopratināšanu vai apcietināšanu.

Valsts tiesību aktos ir paredzēts vispārīgs noteikums, saskaņā ar kuru biometrisko datu apstrāde fiziskas personas unikālas identifikācijas nolūkā ir pieļaujama, ja tas ir absolūti nepieciešams un ja tiek ievērotas atbilstošas garantijas attiecīgās personas tiesībām un brīvībām.

Informācijas avots:

- Datu subjektu veidi: ☒ visas personas
- Attēla avots: ☒ publiski pieejamas telpas ☒ privāta struktūra ☒ citas personas ☒ citi: plašsaziņas līdzekļi.
- Saistība ar noziegumu: ☒ nav obligāti tieša ģeogrāfiska vai laika saistība
- Informācijas iegūšanas veids: ☒ attālināti
- Konteksts — ietekme uz citām pamattiesībām: jā, proti, ☒ pulcēšanās brīvības kontekstā.
- Pieejamie papildu informācijas avoti par datu subjektu:
  ☒ citi: nav izslēgti (piemēram, bankomātu vai veikalu izmantošana), jo nav iespējams kontrolēt motīvus, kas saistīti ar attēliem.

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums: ☒ īpašas datubāzes, kas saistītas ar noziedzības jomu.

Algoritms:

- Apstrādes veids: ☒ pārbaude "viens pret daudziem"

Rezultāti:

- Ietekme: ☒ tieša (piemēram, datu subjekts var tikt arestēts, nopratināts).
- Automatizēts lēmums: ☒ NĒ
- Uzglabāšanas ilgums: līdz tiek izbeigtas visas iespējamās izmeklēšanas

Juridiskā analīze:

- Iepriekšējas informācijas veids datu subjektam: ☒ tiesībaizsardzības iestādes tīmekļvietnē kopumā
- Piemērojamais tiesiskais regulējums: ☒ Tiesībaizsardzības direktīva lielākoties ir kopēta valsts tiesību aktos ☒ vispārīgi valsts tiesību akti par tiesībaizsardzības iestādes biometrisko datu izmantošanu.

3.2. Piemērojamais tiesiskais regulējums

Kā paskaidrots iepriekš, juridiskie pamati, kuros ir tikai atkārtota Tiesībaizsardzības direktīvas 10. panta vispārīgā klauzula, nav pietiekami skaidri formulēti, lai sniegtu personām pietiekamas norādes par nosacījumiem un apstākļiem, kādos tiesībaizsardzības iestādes ir pilnvarotas izmantot videonovērošanas ierakstus no publiskām vietām, lai izveidotu savas sejas biometrisko veidni un salīdzinātu to ar policijas datubāzēm, citiem pieejamiem videonovērošanas vai privātiem ierakstiem utt. Tādēļ šajā scenārijā izveidotais tiesiskais regulējums neatbilst minimālajām prasībām, kas kalpotu par juridisko pamatu.

3.3. Nepieciešamība un samērīgums

Šajā piemērā apstrāde rada dažādas bažas saskaņā ar nepieciešamības un proporcionalitātes principiem vairāku iemeslu dēļ:

personas netiek turētas aizdomās par smagu noziegumu; smagas noziedzīgas uzvedības parādīšana nav priekšnosacījums datņu izmantošanai datubāzē, kas satur attēlu materiālus; arī tieša laika un ģeogrāfiska saistība ar noziegumu nav priekšnoteikums, lai varētu izmantot datubāzē esošās datnes;

tā rezultātā ievērojama daļa vietējo iedzīvotāju tiek glabāta biometriskajā datubāzē, iespējams, vairākus gadus, līdz brīdim, kad visas izmeklēšanas tiek izbeigtas;

nozieguma vietas datubāze neaprobežojas ar attēliem, kas atbilst proporcionalitātes prasībām, tādējādi radot neierobežotu salīdzināmo attēlu skaitu; tas ir pretrunā datu minimizēšanas principam; mazāks attēlu daudzums ļautu apsvērt arī nealgoritmiskus un mazāk uzmācīgus līdzekļus, piemēram, augstas atpazīšanas spējas cilvēkus.[88]

Tā kā piemērs ir redzams no protesta apkārtnes, ir arī iespējams, ka attēli atspoguļo demonstrācijas dalībnieku politiskos uzskatus, jo tā ir otrā īpašā datu kategorija, kas varētu tikt ietekmēta šajā scenārijā. Šajā scenārijā nav skaidrs, kā var novērst šo datu ievākšanu un ar kādiem aizsardzības pasākumiem. Turklāt, ja datu subjekti uzzina, ka viņu dalības demonstrācijā rezultātā viņi ir ievadīti policijas biometriskajā datubāzē, tam var būt nopietna ierobežojoša ietekme uz viņu turpmāko pulcēšanās tiesību īstenošanu.

Datubāzē iekļautās biometriskās veidnes var arī salīdzināt savā starpā. Tas ļauj policijai ne tikai meklēt konkrētu personu visos materiālos, bet arī atkārtoti izveidot personas uzvedības modeli vairāku dienu garumā. Tā var apkopot arī papildu informāciju par personām, piemēram, sociālos kontaktus un politisko līdzdalību.

Ietekmi vēl vairāk pastiprina tas, ka dati tiek apstrādāti bez datu subjektu ziņas.

Ņemot vērā to, ka personas visu laiku ieraksta fotogrāfijas un videomateriālus un ka pat visur esošo videonovērošanas kameras var analizēt biometriski, tas var radīt nopietnu ierobežojošu ietekmi.

Vēl viens iemesls bažām ir privāto fotogrāfiju un videomateriālu plašā izmantošana, tostarp iespējama ļaunprātīga izmantošana, piemēram, denonsēšana. Tā kā ļaunprātīga izmantošana, piemēram, denonsēšana, ir risks, kas raksturīgs arī kriminālprocesam kopumā, risks ir ievērojami lielāks, ņemot vērā apstrādāto datu mērogojamību un iesaistīto personu skaitu, jo cilvēki var augšupielādēt arī materiālus, kas attiecas uz konkrētu personu vai personu grupu, kas viņiem nepatīk. Policijas pieprasījumi augšupielādēt fotogrāfijas un videomateriālus, iespējams, nosaka ļoti zemu slieksni, līdz kuram cilvēki ir gatavi sniegt materiālus, jo īpaši tāpēc, ka to varētu būt iespējams darīt anonīmi vai vismaz bez vajadzības ierasties un identificēties policijas iecirknī.

3.4. Secinājums

Šajā piemērā nav konkrēta noteikuma, kas varētu kalpot par juridisko pamatu. Tomēr, pat ja būtu pietiekams juridiskais pamats, nepieciešamības un samērīguma prasības netiktu izpildītas, tādējādi rastos nesamērīga iejaukšanās datu subjekta tiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību saskaņā ar Hartu.

4 4. SCENĀRIJS

4.1. Apraksts

Policija ievieš veidu, kā identificēt aizdomās turamos, kas izdarījuši smagu noziegumu, kurš fiksēts videonovērošanas kamerās, izmantojot sejas atpazīšanas tehnoloģiju ar atpakaļejošu spēku. Amatpersona manuāli atlasa aizdomās turamo attēlus videomateriālos, kas ievākti no nozieguma vietas vai citas iepriekšējās izmeklēšanas laikā, un pēc tam nosūta attēlu(-us) kriminālistikas dienestam.

[88] T. i., cilvēki ar ārkārtīgi lielu sejas atpazīšanas spēju. Sal. arī: Sejas atpazīšana, ko veic Metropolitēna policijas augstas atpazīšanas spējas cilvēki, 2016. gada 26. februāris, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

Tiesu ekspertīzes dienests izmanto sejas atpazīšanas tehnoloģiju, lai saskaņotu šo(-s) attēlu(-us) ar personu attēliem, ko policija iepriekš apkopojusi datubāzē (t. s. aprakstu datubāze, kurā ir aizdomās turamie un bijušie notiesātie). Apraksta datubāze ir paredzēta šai procedūrai — uz laiku un izolētā vidē — analizē kopā ar sejas atpazīšanas tehnoloģiju, lai varētu veikt saskaņošanas procesu. Lai līdz minimumam samazinātu iejaukšanos saskaņoto personu tiesībās un interesēs, atļauju veikt faktisko saskaņošanas procedūru ir saņēmis ļoti ierobežots skaits tiesu ekspertīžu nodaļas darbinieku, piekļuve datiem ir tikai tiem darbiniekiem, kuriem uzticēta konkrētā lieta, un pirms rezultātu nosūtīšanas izmeklēšanas darbiniekam tiek veikta manuāla rezultātu kontrole. Biometriskie dati netiek nosūtīti ārpus kontrolētās, izolētās vides. Tālāk izmeklēšanā izmanto tikai rezultātu un attēlu (nevis biometrisko veidni). Darbinieki saņem īpašu apmācību par šīs apstrādes noteikumiem un procedūrām, un visa personas un biometrisko datu apstrāde ir pietiekami noteikta valsts tiesību aktos.

Informācijas avots:

- Datu subjektu veidi: ☒ aizdomās turamie, kas identificēti no videonovērošanas ierakstiem.
- Attēla avots: ☒ publiski pieejamas telpas ☒ internets
- Saistība ar noziegumu: ☒ tieša pagaidu
  ☒ tieša ģeogrāfiska
- Informācijas iegūšanas veids: ☒ attālināti
- Konteksts — ietekmē citas pamattiesības: Jā, proti, ☒ pulcēšanās brīvība ☒ vārda brīvība ☒ dažādas: __

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums: ☒ īpašas datubāzes, kas saistītas ar noziedzības jomu.

Algoritms:

- Apstrādes veids: ☒ pārbaude "viens pret daudziem"

Rezultāti:

- Ietekme: ☒ tieša (piemēram, datu subjekts tiek aizturēts, nopratināts)
- Automatizēts lēmums: ☒ NĒ

Juridiskā analīze:

- Piemērojamais tiesiskais regulējums: ☒ šai kompetentajai iestādei piemērojamie īpašie valsts tiesību akti attiecībā uz šo apstrādi (sejas atpazīšana)

4.2. Piemērojamais tiesiskais regulējums

Šajā scenārijā valsts tiesību aktos ir noteikts, ka biometriskos datus var izmantot, veicot kriminālistisko analīzi, ja tas ir absolūti nepieciešams, lai sasniegtu mērķi identificēt aizdomās turamos, kas izdarījuši smagu noziegumu, izmantojot aprakstu datubāzē esošo attēlu salīdzinājumu. Valsts tiesību aktos ir noteikts, kurus datus drīkst apstrādāt, kā arī personas datu integritātes un konfidencialitātes saglabāšanas procedūras un to iznīcināšanas procedūras, tādējādi nodrošinot pietiekamas garantijas pret ļaunprātīgas izmantošanas un patvaļības risku.

4.3. Nepieciešamība un samērīgums

Sejas atpazīšanas izmantošana ir acīmredzami laikietilpīgāka nekā manuāla salīdzināšana kriminālistikas līmenī. Iepriekšēja manuāla attēlu atlase ierobežo iejaukšanos, salīdzinot ar visu video materiālu salīdzināšanu ar datubāzi, un tādējādi tiek diferencētas un atlasītas tikai tās personas, uz kurām attiecas mērķis, t. i., smagu noziegumu apkarošana. Tomēr joprojām ir svarīgi apsvērt, vai

salīdzināšanu var veikt manuāli saprātīgā laikā atkarībā no konkrētā gadījuma. Ierobežojot personu piekļuvi tehnoloģijai un personas datiem, tiek mazināta ietekme uz tiesībām uz privātumu un datu aizsardzību, kā arī biometriskie paraugi netiek glabāti vai izmantoti vēlāk izmeklēšanā. Rezultātu manuāla kontrole arī nozīmē samazinātu jebkādu viltus pozitīvu rezultātu risku.

4.4. Secinājums

Svarīgi, lai valstu tiesību akti nodrošinātu atbilstošu juridisko pamatu biometrisko datu apstrādei, kā arī valsts datubāzei, ar kuru notiek datu salīdzināšana. Šajā scenārijā ir ieviesti vairāki pasākumi, lai ierobežotu iejaukšanos datu aizsardzības tiesībās, piemēram, juridiskajā pamatā noteiktie sejas atpazīšanas tehnoloģijas izmantošanas nosacījumi, to personu skaits, kurām ir piekļuve tehnoloģijai un biometriskajiem datiem, manuālās kontroles u. c. Sejas atpazīšanas tehnoloģija ievērojami uzlabo policijas kriminālistikas nodaļas izmeklēšanas darba efektivitāti, tā ir balstīta uz likumu, kas ļauj policijai apstrādāt biometriskos datus, kad tas ir absolūti nepieciešams, un tāpēc šajās robežās to var uzskatīt par likumīgu iejaukšanos personas tiesībās.

5 5. SCENĀRIJS

5.1. Apraksts

Attālinātā biometriskā identifikācija ir tad, ja personu identitāti nosaka, izmantojot biometriskos identifikatorus (sejas attēlu, gaitu, varavīksneni u. c.), no attāluma, publiskā telpā un nepārtraukti vai pastāvīgi, salīdzinot tos ar (biometriskajiem) datiem, kas glabājas datubāzē[89]. Attālinātā biometriskā identifikācija tiek veikta reāllaikā, ja attēla materiāla uzņemšana, salīdzināšana un identifikācija notiek bez būtiskas kavēšanās.

Pirms katras reāllaika biometriskās attālinātās identifikācijas ieviešanas policija izmeklēšanas ietvaros izveido interesējošo subjektu kontrolsarakstu. Tas ir aizpildīts ar personu sejas attēliem. Pamatojoties uz izlūkdatiem, kas liecina, ka personas atradīsies konkrētā teritorijā, piemēram, iepirkšanās centrā vai publiskā laukumā, policija izlemj, kad, kur un cik ilgi izmantot biometrisko attālināto identifikāciju.

Rīcības dienā viņi novieto policijas furgonu uz zemes kā kontroles centru, kurā atrodas vecākais policijas darbinieks. Furgonā ir monitori, uz kuriem tiek rādīti tuvumā izvietoto to videonovērošanas kameru ieraksti, kas uzstādītas vai nu speciāli, vai pieslēdzoties jau uzstādīto kameru video plūsmām. Kad gājēji iet garām kamerām, tehnoloģija nošķir sejas attēlus, pārvērš tos biometriskajā veidnē un salīdzina ar to personu biometriskajām veidnēm, kas iekļautas kontrolsarakstā.

Ja tiek konstatēta potenciāla sakritība starp kontrolsarakstu un personām, kas šķērso kameras, brīdinājums tiek nosūtīts policistiem furgonā, kuri pēc tam, piemēram, ar radioierīces starpniecību, informē policistus uz vietas, ja brīdinājums ir pozitīvs. Pēc tam darbinieks uz vietas lems par to, vai iejaukties, uzrunāt vai galu galā aizturēt personu. Uz vietas esošā darbinieka veiktie pasākumi tiek reģistrēti. Diskrētas pārbaudes gadījumā tiek saglabāta iegūtā informācija (piemēram, ar ko persona ir kopā, ko tā valkā un uz kurieni dodas).

Minētais valsts tiesību akts paredz vispārīgu noteikumu, saskaņā ar kuru biometrisko datu apstrāde fiziskas personas unikālas identifikācijas nolūkā ir pieļaujama, ja tas ir absolūti nepieciešams un ja tiek ievērotas atbilstošas garantijas attiecīgās personas tiesībām un brīvībām.

Informācijas avots:

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

- Datu subjektu veidi: ☒ visas personas
- Attēla avots: ☒ publiski pieejamas telpas
- Saistība ar noziegumu: ☒ nav obligāti tieša ģeogrāfiska vai laika saistība
- Informācijas iegūšanas veids: ☒ attālināti
- Konteksts — ietekme uz citām pamattiesībām: Jā, proti, ☒ pulcēšanās brīvība ☒ vārda brīvība ☒ dažādas
- Pieejamie papildu informācijas avoti par datu subjektu:
  ☒ citi: nav izslēgti (piemēram, bankomātu vai veikalu izmantošana).

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums: ☒ īpašas datubāzes, kas saistītas ar noziedzības jomu.

Algoritms:

- Apstrādes veids: ☒ pārbaude "viens pret daudziem"

Rezultāti:

- Ietekme: ☒ tieša (piemēram, datu subjekts tiek arestēts, nopratināts).
- Automatizēts lēmums: ☒ NĒ
- Uzglabāšanas ilgums: līdz tiek izbeigtas visas iespējamās izmeklēšanas

Juridiskā analīze:

- Iepriekšējas informācijas veids datu subjektam: ☒ tiesībaizsardzības iestādes tīmekļvietnē kopumā
- Piemērojamais tiesiskais regulējums: ☒ Tiesībaizsardzības direktīva lielākoties kopēta ar valsts tiesību aktos ☒ vispārīgi valsts tiesību akti par tiesībaizsardzības iestādes biometrisko datu izmantošanu.

5.2. Piemērojamais tiesiskais regulējums

Juridiskie pamati, kas tikai atkārto Tiesībaizsardzības direktīvas 10. panta vispārējo klauzulu, nav pietiekami skaidri to izteiksmē, lai sniegtu personām pienācīgu norādi par nosacījumiem un apstākļiem, kādos tiesībaizsardzības iestādēm ir tiesības izmantot videonovērošanas kameru ierakstus no publiskām vietām, lai izveidotu savas sejas biometrisko veidni, un salīdzinātu to ar policijas datubāzēm. Tāpēc šajā scenārijā izveidotais tiesiskais regulējums neatbilst minimālajām prasībām, lai kalpotu par juridisko pamatu.[90]

5.3. Nepieciešamība un samērīgums

Jo lielāka iejaukšanās jo nepieciešamības un proporcionalitātes robežlīmenis kļūst augstāks. Attālināta biometriskā identifikācija sabiedriskās vietās ietekmē vairākas pamattiesības:

scenāriji ietver katra garāmgājēja novērošanu attiecīgajā publiskajā telpā; tādējādi tas nopietni ietekmē iedzīvotāju pamatotās cerības uz anonimitāti publiskās vietās[91]; tas ir priekšnoteikums daudziem demokrātiskā procesa aspektiem, piemēram, lēmumam iestāties pilsoniskajā apvienībā, apmeklēt sapulces un tikties ar dažādu sociālo un kultūras slāņu cilvēkiem, piedalīties politiskos protestos un apmeklēt visdažādākās vietas. Anonimitātes jēdziens sabiedriskās vietās ir būtisks, lai brīvi

[90] Gadījumos, kad zinātniskam projektam, kura mērķis ir izpētīt sejas atpazīšanas tehnoloģijas izmantošanu, būtu jāapstrādā personas dati, bet uz šādu apstrādi neattiektos Tiesībaizsardzības direktīvas 4. panta 3. punkts vai tā neietilptu Savienības tiesību aktu darbības jomā, būtu piemērojama VDAR. Tādu izmēģinājuma projektu gadījumā, kuriem sekotu tiesībaizsardzības pasākumi, joprojām būtu piemērojama Tiesībaizsardzības direktīva.

[91] EDAK atbilde Eiropas Parlamenta deputātiem par sejas atpazīšanas lietotni, ko izstrādājusi "Clearview AI", 2020. gada 10. jūnijs, ats.: OUT2020-0052.

ievāktu informāciju un idejas un apmainītos ar tām. Tas saglabā viedokļu pluralitāti, mierīgas pulcēšanās brīvību un biedrošanās brīvību, kā arī minoritāšu aizsardzību un atbalsta varas dalīšanas, pārbaužu un līdzsvara principus. Anonimitātes jēdziena vājināšana sabiedriskās vietās var radīt spēcīgu atturošu ietekmi uz iedzīvotājiem. Viņi var atturēties no noteiktas rīcības, kas ir brīvas un atvērtas sabiedrības kompetencē. Tas ietekmētu sabiedrības intereses, jo demokrātiskai sabiedrībai ir nepieciešama tās pilsoņu pašnoteikšanās un līdzdalība demokrātiskajā procesā.

Ja šāda tehnoloģija tiks pielietota, tad, vienkārši ejot pa ielu, dodoties uz metro vai uz maiznīcu skartajā teritorijā, tiesībaizsardzības iestādes vāks personas, tostarp biometriskos datus un, pirmajā gadījumā, arī salīdzinās ar policijas datubāzēm. Situācija, kad tas notiktu, noņemot pirkstu nospiedumus, būtu acīmredzami nesamērīga.

Ietekmēto datu subjektu skaits ir ārkārtīgi liels, jo tiek ietekmēts ikviens, kas iet garām attiecīgajai publiskai vietai. Turklāt scenāriji nozīmētu automatizētu biometrisko datu masveida apstrādi, kā arī biometrisko datu masveida salīdzināšanu ar policijas datubāzēm.

Visā Eiropas judikatūrā ir aizliegta masveida novērošana (piemēram, ECT lietā S. un Marper pret Apvienoto Karalisti uzskatīja, ka neselektīva biometrisko datu saglabāšana ir "nesamērīga iejaukšanās" tiesībās uz privātumu, jo tā nav uzskatāma par "vajadzīgu demokrātiskā sabiedrībā").

Attālinātā biometriskā identifikācija ir tik pakļauta masveida uzraudzībai, ka nav uzticamu ierobežošanas līdzekļu. Tas būtībā atšķiras no videonovērošanas kā tādas, jo videoierakstu iespējamā izmantošana bez biometriskās identifikācijas jau ir spēcīga iejaukšanās, bet vienlaikus ierobežota, savukārt sejas atpazīšanas tehnoloģijas piemērošanas gadījumā jau plaši izplatītā videonovērošanas sistēma kā galvenais datu avots mainīsies kvalitātē. Turklāt, jo īpaši attiecībā uz iecerēto ierobežojošo ietekmi, iespējamie ierobežojumi jau esošo videonovērošanas iekārtu piemērošanā nebūs redzami, un tādējādi sabiedrība tiem neuzticēsies.

Neklātienes biometriskā identifikācija, ko veic policijas iestādes, uzskata ikvienu par iespējamu aizdomās turamo. Tomēr tiesiskā valstī pilsoņi tiek uzskatīti par taisnīgiem, kamēr nav pierādīts viņu pārkāpums. Šis principu daļēji tiek atspoguļots arī Tiesībaizsardzības direktīvā, kurā tiek uzsvērta nepieciešamība, cik vien iespējams, nošķirt attieksmi pret notiesātajiem vai aizdomās turētamajiem, un šajā gadījumā tiesībaizsardzības iestādēm ir jābūt "*nopietnam pamatam, lai uzskatītu, ka viņi ir izdarījuši vai gatavojas izdarīt noziedzīgu nodarījumu*" (Tiesībaizsardzības direktīvas 6. panta a) punkts), salīdzinot ar personām, kuras nav notiesātas vai turētas aizdomās par noziedzīgu darbību.

To piemēro transporta mezgla punktiem vai sabiedriskām vietām, jo tiesībaizsardzības iestādes izmanto tehnoloģiju, kas spēj unikāli identificēt vienu personu un izsekot un analizēt tās atrašanās vietu un pārvietošanās atklās vissensitīvāko informāciju par personu (pat seksuālās preferences, reliģiju, veselības problēmas). Līdz ar to pastāv milzīgs risks saistībā ar nelikumīgu piekļuvi datiem un to izmantošanu.

Tādas sistēmas uzstādīšana, kas ļauj atklāt personas uzvedības un īpašību kodolu, rada spēcīgu ierobežojošu ietekmi. Tas liek cilvēkiem šaubīties par to, vai pievienoties noteiktai izpausmei, tādējādi kaitējot demokrātiskajam procesam. Arī tikšanās un atrašanās sabiedrībā kopā ar kādu draugu, par kuru zināms, ka viņam ir problēmas ar policiju vai kurš uzvedas savdabīgi, var tikt uzskatīta par kritisku, jo tas viss varētu piesaistīt sistēmas algoritmu un līdz ar to arī tiesībaizsardzības iestādes.

Nav iespējams aizsargāt neaizsargātus datu subjektus, piemēram, bērnus. Turklāt tiek ietekmētas personas, kurām ir profesionāla interese un bieži atbilstošs juridisks pienākums ievērot savu kontaktu konfidencialitāti, piemēram, žurnālisti, juristi un garīdznieki. Tas varētu, piemēram, novest pie avota

un žurnālista atklāšanas vai pie tā, ka persona konsultējas ar krimināllietu advokātu. Problēma attiecas ne tikai uz nejaušām sabiedriskām vietām, kur tiekas, piemēram, žurnālisti un viņu avoti, bet, protams, arī uz sabiedriskām vietām, kas vajadzīgas, lai šajā sakarā vērstos pie iestādēm vai profesionāļiem un piekļūtu tām.

Turklāt cilvēku diskomforts, ko rada sejas atpazīšanas tehnoloģija, var izraisīt to, ka viņi maina savu uzvedību, izvairās no vietām, kur sejas atpazīšanas tehnoloģija ir izvietota, un tādējādi atsakās no sociālās dzīves un kultūras pasākumiem. Atkarībā no sejas atpazīšanas tehnoloģijas izvēršanas apmēra ietekme uz cilvēkiem var būt tik nozīmīga, ka ietekmēt viņu spēju dzīvot cilvēka cienīgu dzīvi[92].

Tāpēc pastāv liela iespēja ietekmēt tiesību uz personas datu aizsardzību būtību, neaizskaramo pamatu. Spēcīgas norādes (sal. pamatnostādņu 3.1.3.2. sadaļa) ir jo īpaši šādas: tiesībaizsardzības iestādes plašā mērogā automātiski apstrādā cilvēku unikālās bioloģiskās pazīmes, izmantojot algoritmus, kas balstīti uz ticamību, un rezultātu izskaidrojamība ir tikai ierobežota. Tiesību uz privātumu un datu aizsardzību ierobežojumi tiek piemēroti neatkarīgi no personas individuālās rīcības vai apstākļiem, kas uz to attiecas. Gandrīz visi datu subjekti, kurus ietekmē šī iejaukšanās, statistiski ir fiziskas personas, kuras ievēro likumus. Pastāv tikai ierobežotas iespējas sniegt informāciju datu subjektam. Vairumā gadījumu pārsūdzība tiesā būs iespējama tikai pēc tam.

Paļaušanās uz sistēmu, kas balstīta uz ticamību un ar ierobežotu izskaidrojamību, var izraisīt atbildības izplatīšanos un trūkumu tiesiskās aizsardzības jomā, kā arī var būt stimuls nolaidībai.

Tiklīdz šāda sistēma, ko var piemērot arī esošajām videonovērošanas kamerām, tiek piemērota, to var izmantot ļaunprātīgi, bez lielām pūlēm un personām neredzot, un tā ļauj sistemātiski un ātri izveidot cilvēku sarakstus pēc etniskās izcelsmes, dzimuma, reliģijas utt. Personas datu apstrādes princips, pamatojoties uz iepriekš noteiktiem kritērijiem, piemēram, personas atrašanās vietu un nobraukto maršrutu, jau tiek praktizēts[93] un ir pakļauts diskriminācijai.

Ņemot vērā sensitivitāti, izteiksmi un apstrādāto datu daudzumu, sistēmas sejas atpazīšanai no attāluma publiski pieejamās vietās var tikt izmantotas ļaunprātīgi, radot negatīvas sekas attiecīgajām personām. Šādus datus var arī viegli ievākt un ļaunprātīgi izmantot, lai izdarītu spiedienu uz galvenajiem kontroles un līdzsvara principa dalībniekiem, piemēram, politisko opozīciju, amatpersonām un žurnālistiem.

Visbeidzot, sejas atpazīšanas tehnoloģijas sistēmas parasti ietver spēcīgu aizspriedumu efektu attiecībā uz rasi un dzimumu: nepatiesi pozitīvi rezultāti nesamērīgi ietekmē ādas krāsas cilvēkus un sievietes[94],izraisot diskrimināciju. Policijas pasākumi pēc viltus pozitīvu rezultātu iegūšanas, piemēram, kratīšanas un aresti, vēl vairāk stigmatizē šīs grupas.

5.4. Secinājums

Iepriekš minētie scenāriji attiecībā uz biometrisko datu attālinātu apstrādi sabiedriskās vietās identifikācijas nolūkos nenodrošina taisnīgu līdzsvaru starp konkurējošām privātajām un publiskajām

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

[93] Sal. Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/681 (2016. gada 27. aprīlis) par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem, 6. pants, un Eiropas Parlamenta un Padomes Regulas (ES) 2018/1240 (2018. gada 12. septembris), ar ko izveido Eiropas ceļošanas informācijas un atļauju sistēmu (ETIAS) un groza Regulas (ES) Nr. 1077/2011, (ES) Nr. 515/2014, (ES) 2016/399, (ES) 2016/1624 un (ES) 2017/2226, 33. pants.

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

interesēm, tādējādi radot nesamērīgu iejaukšanos datu subjekta tiesībās saskaņā ar Hartas 7. un 8. pantu.

6 6. SCENĀRIJS

6.1. Apraksts

Privāta struktūra nodrošina lietojumprogrammu, kurā sejas attēli tiek noskrāpēti internetā, lai izveidotu datubāzi. Pēc tam lietotājs, piemēram, policija, var augšupielādēt attēlu, un, izmantojot biometrisko identifikāciju, lietojumprogramma mēģinās to saskaņot ar sejas attēliem vai biometriskajiem šabloniem, kas atrodas tās datubāzē.

Vietējā policijas nodaļa veic izmeklēšanu par videoierakstā fiksētu noziegumu, kurā nav iespējams identificēt vairākus iespējamos lieciniekus un aizdomās turamos, salīdzinot ievākto informāciju ar iekšējām datubāzēm vai izlūkdatiem. Pamatojoties uz ievākto informāciju, šīs personas nav reģistrētas nevienā esošajā policijas datubāzē. Policija nolemj izmantot iepriekš aprakstīto rīku, ko nodrošina privāts uzņēmums, lai identificētu personas, izmantojot biometrisko identifikāciju.

Informācijas avots:

- Datu subjektu veidi: ☒ visi iedzīvotāji (liecinieki) ☒ notiesātie ☒ aizdomās turamie
- Attēla avots: ☒ videomateriāls no publiskas vietas vai citur savākts iepriekšējas izmeklēšanas laikā.
- Saistība ar noziegumu: ☒ nav nepieciešams
- Informācijas iegūšanas veids: ☒ attālināti
- Konteksts — ietekme uz citām pamattiesībām: Jā, proti, ☒ pulcēšanās brīvība ☒ vārda brīvība ☒ dažādi: __

Atsauces datubāze (ar kuru salīdzina iegūto informāciju):

- Specifiskums: ☒ vispārējas nozīmes datubāzes, kas aizpildītas no interneta

Algoritms:

- Apstrādes veids: ☒ pārbaude "viens pret daudziem"

Rezultāti:

- Ietekme ☒ tieša (piemēram, datu subjekts tiek arestēts, nopratināts, diskriminējoša uzvedība)
- Automatizēts lēmums: ☒ NĒ

Juridiskā analīze:

- Iepriekšējas informācijas veids datu subjektam: ☒ Nē

6.2. Piemērojamais tiesiskais regulējums

Ja privāta struktūra sniedz pakalpojumu, kas ietver personas datu apstrādi, kuras mērķi un līdzekļus nosaka tā pati (šajā gadījumā attēlu izgriešana no interneta, lai izveidotu datubāzi), šai privātai struktūrai ir jābūt juridiskam pamatojumam šādai apstrādei. Turklāt tiesībaizsardzības iestādei, kas nolemj izmantot šo pakalpojumu saviem mērķiem, ir jābūt tiesiskajam pamatojumam apstrādei, kurai tā nosaka nolūkus un līdzekļus. Lai tiesībaizsardzības iestāde varētu apstrādāt biometriskos datus, ir vajadzīgs tiesiskais regulējums, kas nosaka mērķi, apstrādājamos personas datus, apstrādes nolūkus

un procedūras personas datu integritātes un konfidencialitātes saglabāšanai, kā arī to iznīcināšanas procedūras.

Šis scenārijs paredz personas datu masveida ievākšanu no personām, kuras nav informētas par to, ka tiek ievākti viņu dati. Šāda apstrāde varētu būt likumīga tikai ļoti ārkārtējos apstākļos. Atkarībā no tā, kur datubāze atrodas, izmantojot šādu pakalpojumu, var būt nepieciešama personas datu un/vai īpašu kategoriju personas datu nosūtīšana ārpus Eiropas Savienības (policija, piemēram, "nosūta" sejas attēlu novērošanas video vai kas citādi ievākts), tādējādi pieprasot īpašus nosacījumus šādai pārsūtīšanai, skat. Tiesībaizsardzības direktīvas 39. pantu.

Šajā scenārijā nav īpašu noteikumu, kas ļautu tiesībaizsardzības iestādei veikt šādu apstrādi.

6.3. Nepieciešamība un samērīgums

Tas, ka tiesībaizsardzības iestāde izmanto pakalpojumu, nozīmē, ka personas dati tiek kopīgoti ar privātu struktūru, kas izmanto datubāzi, kurā personas dati tiek ievākti neierobežoti un masveidā. Starp ievāktajiem personas datiem un tiesībaizsardzības iestādes izvirzīto mērķi nav nekādas saistības. Tiesībaizsardzības iestādes veiktā datu apmaiņa ar privāto struktūru nozīmē arī to, ka iestādei nav kontroles pār datiem, ko apstrādā privātā struktūra, un datu subjektiem ir lielas grūtības īstenot savas tiesības, jo tie nezinās, ka viņu dati tiek apstrādāti šādā veidā. Tas nosaka ļoti augstu latiņu situācijās, kad šāda apstrāde vispār varētu notikt. Apšaubāms, vai kāds mērķis atbilstu direktīvā noteiktajām prasībām, jo jebkādas atkāpes no tiesībām uz privāto dzīvi un datu aizsardzību un to ierobežojumi ir piemērojami tikai tad, ja tas ir absolūti nepieciešams. Vispārējās efektivitātes intereses smagu noziegumu apkarošanā pašas par sevi nevar attaisnot apstrādi, ja šādi milzīgi datu apjomi tiek vākti bez izšķirības. Tādējādi šī apstrāde neatbilstu nepieciešamības un proporcionalitātes prasībām.

6.4. Secinājums

Tā kā nav skaidru, precīzu un paredzamu noteikumu, kas atbilstu direktīvas 4. un 10. panta prasībām, un nav pierādījumu, ka šī apstrāde ir absolūti nepieciešama, lai sasniegtu paredzētos mērķus, var secināt, ka šīs lietojumprogrammas izmantošana neatbilstu nepieciešamības un proporcionalitātes prasībām un nozīmētu nesamērīgu iejaukšanos datu subjektu tiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību saskaņā ar Hartu.