

Suunised



**Suunised 05/2022 näotuvastustehnoloogia kasutamise
kohta õiguskaitse valdkonnas**

Version 2.0.

Vastu võetud 26. aprillil 2023

Versiooniajalugu

Versioon 1.0	12. mai 2022	Suuniste vastuvõtmine avalikuks konsulteerimiseks
Versioon 2.0.	26. aprill 2023	Suuniste vastuvõtmine pärast avalikku konsulteerimist

Sisukord

Kommenteeritud kokkuvõte	5
1 Sissejuhatus	8
2 Tehnoloogia	9
2.1 Üks biomeetriline tehnoloogia, kaks erinevat funktsiooni	9
2.2 Mitmesugused eesmärgid ja rakendused	10
2.3 Usaldusväärsus, täpsus ja ohud andmesubjektidele	12
3 Kohaldatav õigusraamistik	13
3.1 Üldine õigusraamistik – ELi põhiõiguste harta ja Euroopa inimõiguste ja põhivabaduste kaitse konventsioon	13
3.1.1 Harta kohaldatavus	14
3.1.2 Sekkumine hartas sätestatud õigustesse	14
3.1.3 Sekkumise õigustus	15
3.2 Konkreetne õigusraamistik - õiguskaitse direktiiv	19
3.2.1 Andmete eriliikide töötlemine õiguskaitse eesmärgil	20
3.2.2 Automatiseeritud töötlusel põhinevate üksikotsuste tegemine, sealhulgas profiilianalüüs	22
3.2.3 Andmesubjektide kategooriad	22
3.2.4 Andmesubjekti õigused	23
3.2.5 Muud õiguslikud nõuded ja kaitsemeetmed	26
4 Järeldus	29
5 Lisad	29
I lisa. Stsenaariumide kirjeldamise vorm	30
II lisa. Praktilised suunised näotuvastustehnoloogia projektide juhtimiseks õiguskaitseasutustes	32
1. ÜLESANDED JA KOHUSTUSED	32
2. ALGETAPP / ENNE NÄOTUVASTUSTEHNOLOOGIA SÜSTEEMI HANKIMIST	33
3. NÄOTUVASTUSTEHNOLOOGIA HANKEETAPIS JA ENNE KASUTUSELEVÕTTU	35
4. SOOVITUSED PÄRAST NÄOTUVASTUSTEHNOLOOGIA KASUTUSELEVÕTTU	37
III lisa. PRAKTILISED NÄITED	38
1. 1. stsenaarium	38
1.1. Kirjeldus	38
1.2. Kohaldatav õigusraamistik	39
1.3. Vajalikkus ja proportsionaalsus – kuriteo eesmärk/raskusaste	39
1.4. Järeldus	40
2. 2. stsenaarium	40

2.1.	Kirjeldus.....	40
2.2.	Kohaldatav õigusraamistik	41
2.3.	Vajalikkus ja proportsionaalsus – kuriteo eesmärk / raskusaste / mitteseotud isikute arv, keda töötlemine mõjutab	41
2.4.	Järeldus	42
3	3. stsenaarium	42
3.1.	Kirjeldus.....	42
3.2.	Kohaldatav õigusraamistik	43
3.3.	Vajalikkus ja proportsionaalsus.....	43
3.4.	Järeldus	44
4	4. stsenaarium	44
4.1.	Kirjeldus.....	44
4.2.	Kohaldatav õigusraamistik	45
4.3.	Vajalikkus ja proportsionaalsus.....	45
4.4.	Järeldus	46
5	5. stsenaarium	46
5.1.	Kirjeldus.....	46
5.2.	Kohaldatav õigusraamistik	47
5.3.	Vajalikkus ja proportsionaalsus.....	47
5.4.	Järeldus	49
6	6. stsenaarium	50
6.1.	Kirjeldus.....	50
6.2.	Kohaldatav õigusraamistik	50
6.3.	Vajalikkus ja proportsionaalsus.....	51
6.4.	Järeldus	51

KOMMENTEERITUD KOKKUVÕTE

Üha enam õiguskaitseasutusi kasutab või kavatseb kasutada näotuvastustehnoloogiat. Seda võib kasutada isiku **autentimiseks** või **tuvastamiseks** ning seda saab kohaldada videotele (nt videovalvele) või fotodele. Seda võib kasutada eri eesmärkidel, sealhulgas politsei jälgimisnimekirjades olevate isikute otsimiseks või isiku liikumise jälgimiseks avalikus kohas.

Näotuvastustehnoloogia põhineb **biomeetriliste andmete** töötlemisel, hõlmates seega isikuandmete eriliikide töötlemist. Sageli kasutab näotuvastustehnoloogia **tehisintellekti** või masinõppe komponente. Kuigi see tehnoloogia võimaldab suuremahulist andmetöötlust, kaasneb sellega ka diskrimineerimise ja valetulemuste risk. Näotuvastustehnoloogiat võib kasutada kontrollitud „üks-ühele“ olukordades, kuid ka väga suurtes rahvahulkades ja transpordisõlmedes.

Näotuvastustehnoloogia on **õiguskaitseasutuste jaoks tundlik vahend**. Õiguskaitseasutused on täidesaatsva riigivõimu asutused ja nad on sõltumatud . Näotuvastustehnoloogiaga on võimalik sekkuda põhiõigustesse – mitte ainult õigusesse isikuandmete kaitsele – ning see võib mõjutada meie ühiskondlikku ja demokraatlikku poliitilist stabiilsust.

Isikuandmete kaitse tagamiseks õiguskaitse kontekstis peavad olema täidetud **õiguskaitseDirektiivi nõuded**. ÕiguskaitseDirektiiv sätestab teatud raamistiku näotuvastustehnoloogia kasutamiseks, eelkõige artikli 3 lõikes 13 (mõiste „biomeetrilised andmed“), artiklis 4 (isikuandmete töötlemise põhimõtted), artiklis 8 (töötlemise seaduslikkus), artiklis 10 (isikuandmete eriliikide töötlemine) ja artiklis 11 (automatiseeritud töötlusel põhinevate üksikotsuste tegemine).

Näotuvastustehnoloogia kasutamine võib mõjutada ka mitut muud põhiõigust. Seetõttu on õiguskaitseDirektiivi tõlgendamisel oluline **ELi põhiõiguste harta** (edaspidi „harta“), eelkõige harta artiklis 8 sätestatud õigus isikuandmete kaitsele, aga ka harta artiklis 7 sätestatud õigus era- ja perekonnaelu austamisele.

Isikuandmete töötlemise õiguslikuks aluseks olevad **seadusandlikud meetmed** riivavad otseselt harta artiklitega 7 ja 8 tagatud õigusi. Biomeetriliste andmete töötlemine on igas olukorras iseenesest tõsine sekkumine. See ei sõltu tulemusest, nt positiivsest kokkulangevusest. Kõik põhiõiguste ja -vabaduste teostamise piirangud peavad olema sätestatud seaduses ning austama nende õiguste ja vabaduste olemust.

Õiguslik alus peab olema **piisavalt selge** ja andma kodanikele piisavat teavet tingimuste ja asjaolude kohta, mille korral on ametiasutustel õigus kasutada andmete kogumise ja salajase jälgimise meetmeid. Pelgalt õiguskaitseDirektiivi artikli 10 üldise sätte ülevõtmisega siseriiklikkusse õigusesse puudusid täpsus ja ettenähtavus.

Enne kui riigi seadusandja loob uue õigusliku aluse näotuvastustehnoloogiaga biomeetriliste andmete mis tahes töötlemiseks , tuleks **konsulteerida** pädeva andmekaitse järelevalveasutusega.

Seadusandlikud meetmed peavad olema asjaomaste õigusaktide õiguspärase eesmärkide saavutamiseks **sobivad**. **Üldist huvi pakkuv eesmärk** – kui kaalukas tahes – ei õigusta iseenesest põhiõiguse piiramist. Seadusandlikud meetmed peaksid eristama ja olema suunatud isikutele, kelle suhtes neid kohaldatakse, pidades silmas konkreetset eesmärki, nt raskete kuritegude vastast võitlust. Kui meede hõlmab isikuid üldiselt ilma eristamise, piiramise või erandite kohaldamiseta, suurendab see sekkumist. Samuti suurendab see sekkumist, kui andmetöötlus hõlmab märkimisväärt osa elanikkonnast.

Andmeid tuleb töödelda viisil, mis tagab ELi andmekaitse eeskirjade ja põhimõtete kohaldatavuse ja tõhususe. Vastavalt olukorrale tuleb **vajalikkuse ja proportsionaalsuse hindamisel** tuvastada ja kaaluda ka kõiki võimalikke mõjusid teistele põhiõigustele. Kui andmeid töödeldakse süstemaatiliselt ilma andmesubjektide teadmata, tekitab see tõenäoliselt **üldise tunde**, et ollakse **pideva jälgimise all**. Sel võib olla heidutav mõju teatud põhiõiguste või kõikide põhiõiguste kasutamisele, nagu inimväärikus vastavalt harta artiklile 1, mõtte-, südametunnistuse- ja usuvabadus vastavalt harta artiklile 10, sõnavabadus vastavalt harta artiklile 11 ning kogunemis- ja ühinemisvabadus vastavalt harta artiklile 12.

Andmete eriliikide, nt biomeetriliste andmete töötlemist saab pidada **rangelt vajalikuks** (õiguskaitseDirektiivi artikkel 10) üksnes siis, kui isikuandmete kaitsesse sekkumine ja selle piirangud piirduvad vaid hädavajalikuga ning ei hõlma üldist või süstemaatilist laadi töötlemist.

Asjaolu, et andmesubjekt on foto **ilmselt avalikustanud** (õiguskaitseDirektiivi artikkel 10), ei tähenda, et sellega seotud biomeetrilised andmed, mida saab fotost konkreetsete tehniliste vahenditega välja võtta, loetakse ilmselt avalikustatuks. Teenuse vaikeseadistusi, näiteks mallide avalikustamist, või valikuvõimaluse puudumist, näiteks mallide avalikustamist ilma, et kasutaja saaks seda seadet muuta, ei tohiks mingil juhul tõlgendada kui andmete ilmselt avalikustamist.

ÕiguskaitseDirektiivi artikliga 11 kehtestatakse raamistik **automatiseeritud töötlusel põhinevate üksikotsuste tegemiseks**. Näotuvastustehnoloogia kasutamine hõlmab andmete eriliikide kasutamist ning võib tingida profiilialüüsi tegemise, olenevalt sellest, kuidas ja mis eesmärgil näotuvastustehnoloogiat rakendatakse. Igal juhul on vastavalt liidu õigusele ja õiguskaitseDirektiivi artikli 11 lõikele 3 keelatud profiilialüüs, mille tulemusel füüsilisi isikuid diskrimineeritakse isikuandmete eriliikide alusel.

ÕiguskaitseDirektiivi artikkel 6 käsitleb **andmesubjektide eri kategooriate eristamise** vajadust. Kui andmesubjektide kohta puuduvad tõendid, et nende käitumisel võiks olla kasvõi kaudne seos õiguskaitseDirektiivi kohase õiguspärase eesmärgiga, ei ole sekkumine tõenäoliselt põhjendatud.

Võimalikult väheste andmete kogumise põhimõte (õiguskaitseDirektiivi artikli 4 lõike 1 punkt e) nõuab samuti, et igasugune videomaterjal, mis ei ole töötlemise eesmärgi seisukohalt asjakohane, tuleks alati enne kasutamist eemaldada või anonüümiseerida (nt hägustades, ilma et andmeid oleks võimalik tagasiulatuvalt taastada).

Vastutav töötleja peab enne näotuvastustehnoloogial põhinevat mis tahes töötlemistoimingut hoolikalt kaaluma, kuidas (või kas on võimalik) täita **andmesubjekti õiguste** nõudeid, sest näotuvastustehnoloogia hõlmab sageli isikuandmete eriliikide töötlemist ilma andmesubjektiga mingil viisil suhtlemata.

Andmesubjekti õiguste tõhus kasutamine sõltub sellest, kas vastutav töötleja täidab oma **teavitamiskohustusi** (õiguskaitseDirektiivi artikkel 13). Kui hinnatakse, kas on olemas õiguskaitseDirektiivi artikli 13 lõike 2 kohane „konkreetne juhtum“, tuleb arvestada mitmeid tegureid, sealhulgas kas isikuandmeid kogutakse andmesubjekti teadmata, sest see oleks ainus viis, kuidas andmesubjektid saaksid oma õigusi tõhusalt kasutada. Kui otsused tehakse üksnes näotuvastustehnoloogia põhjal, tuleb andmesubjekte teavitada automatiseeritud töötlusel põhinevate otsuste tegemise protsessist.

Mis puudutab **andmetega tutvumise taotlusi**, siis kui biomeetrilised andmed on salvestatud ja identiteediga seostatud ka tähtnumbriliste andmete abil, peaks see kooskõlas võimalikult väheste andmete kogumise põhimõttega võimaldama pädeval asutusel kinnitada tutvumistaotluse vaid nende

tähtnumbriliste andmete otsingu põhjal, alustamata isikute muude biomeetriliste andmete edasist töötlust (st näotuvastustehnoloogial põhinev otsing andmebaasis).

Riskid andmesubjektidele on eriti suured, kui ebaõigeid andmeid säilitatakse politsei andmebaasis ja/või jagatakse teiste üksustega. Vastutav töötleja peab säilitatud andmeid ja näotuvastussüsteeme vastavalt **korrigeerima** (vt ka õiguskaitseDirektiivi põhjendus 47).

Piiramise õigus on eriti oluline, kui näotuvastustehnoloogiat (mis põhineb algoritmi(de)l ja ei anna seega kunagi lõplikku tulemust) kasutatakse olukordades, kus kogutakse suuri hulki andmeid ning tuvastamise täpsus ja kvaliteet võivad varieeruda.

Andmekaitsealase mõjuhinna tegemine enne näotuvastustehnoloogiat kasutamist on kohustuslik nõue (vt õiguskaitseDirektiivi artikkel 27). Euroopa AndmekaitseNõukogu (edaspidi „EDPB“) soovib usalduse ja läbipaistvuse suurendamise meetmena avalikustada selliste hinnangute tulemused või vähemalt peamised järeldused.

Enamik näotuvastustehnoloogia rakendamise ja kasutamise juhtumeid sisaldavad suurt ohtu andmesubjektide õigustele ja vabadustele. Seetõttu peaks näotuvastustehnoloogiat rakendav asutus **konsulteerima** enne süsteemi kasutuselevõttu pädeva järelevalveasutusega.

Biomeetriliste andmete ainulaadset olemust arvestades peaks näotuvastustehnoloogiat rakendav ja/või kasutav asutus pöörama kooskõlas õiguskaitseDirektiivi artikliga 29 erilist tähelepanu **töötlemise turvalisusele**. Eelkõige peaks õiguskaitseasutus tagama, et süsteem vastaks asjakohastele standarditele, ja rakendama biomeetriliste mallidelle kaitsemeetmeid. Andmekaitse põhimõtted ja kaitsemeetmed peavad olema tehnoloogiasse loimitud enne isikuandmete töötlemise algust. Seega isegi juhul, kui õiguskaitseasutus kavatseb kohaldada ja kasutada välise teenuseosutajate pakutavat näotuvastustehnoloogiat, peab ta tagama, näiteks läbi hankemenetluse, et kasutusele võetaks üksnes **loimitud ja vaikimisi andmekaitse** põhimõtetele vastav näotuvastustehnoloogia.

Logimine (vt õiguskaitseDirektiivi artikkel 25) on oluline kaitsemeede töötlemise õiguspärasuse kontrollimiseks nii asutusesiseselt (st asjaomase vastutava töötleja / volitatud töötleja sisekontroll) kui ka välise järelevalveasutuste poolt. Näotuvastussüsteemide kontekstis on soovitatav logida ka muudatusi võrdlusandmebaasis ning identifitseerimis- või verifitseerimiskatseid, sealhulgas kasutajat, tulemust ja usaldusnäitajat. Logimine on aga vaid üks üldise **vastutuse põhimõtte** olulisi elemente (vt õiguskaitseDirektiivi artikli 4 lõige 4). Vastutav töötleja peab olema võimeline tõendama, et töötlemine on kooskõlas õiguskaitseDirektiivi artikli 4 lõigetes 1–3 sätestatud isikuandmete kaitse aluspõhimõtetega.

EDPB tuleb meelde enda ja Euroopa Andmekaitseinspektori ühist **üleskutset keelata** teatavat liiki töötlemistoimingud: 1) isikute biomeetriline kaugtuvastus avalikes kohtades, 2) tehisintellektipõhised näotuvastussüsteemid, mis liigitavad isikuid nende biomeetriliste andmete alusel etnilise päritolu, soo, poliitiliste veendumuste, seksuaalse sättumuse või muude diskrimineerimise põhjuste järgi klastritesse, 3) näotuvastuse või sarnaste tehnoloogiate kasutamine füüsiliste isikute emotsioonide järeldamiseks ja 4) õiguskaitse kontekstis toimuv isikuandmete töötlemine, mis põhineb andmebaasil, mis on täidetud massiliselt ja valimatult, näiteks internetist fotode ja näopiltide „koorimise“ teel kogutud isikuandmetega.

Põhiõiguste keskne kaitsemeede on **tõhus järelevalve** pädevate andmekaitse järelevalveasutuste poolt. Seetõttu peavad liikmesriigid tagama, et järelevalveasutuste ressursid oleks asjakohased ja piisavad, et nad saaksid oma volitusi täita.

Need **suunised on adresseeritud** ELi ja riikide tasandil seadusandjatele, samuti õiguskaitseasutustele ja ametnikele, kes näotuvastussüsteeme rakendavad ja kasutavad. Need on adresseeritud üksikisikutele sedavõrd, kui nad on üldiselt või andmesubjektidena teemast huvitatud, eelkõige seoses andmesubjektide õigustega.

Suuniste eesmärk on anda teavet näotuvastustehnoloogia teatud omadustest ja kohaldatavast õigusraamistikust õiguskaitse kontekstis (eelkõige õiguskaitse direktiiv).

- Lisaks on need suunised **konkreetses kasutusjuhtumi tundlikkuse esmase klassifikatsiooni toetamise vahend (I lisa)**.
- Samuti pakuvad need **praktilisi juhiseid õiguskaitseasutustele, kes soovivad näotuvastussüsteemi hankida ja käitada (II lisa)**.
- Suunistes kirjeldatakse ka mitmeid tüüpilisi **kasutusjuhtumeid ja esitatakse mitmed asjakohased kaalutlused**, eelkõige seoses vajalikkuse ja proportsionaalsuse testiga (III lisa).

1 SISSEJUHATUS

1. Näotuvastustehnoloogiat võib kasutada isikute automaatseks tuvastamiseks nende näo põhjal. Näotuvastustehnoloogia põhineb sageli tehisintellektil, näiteks masinõppe tehnoloogiatel. Näotuvastustehnoloogia rakendusi katsetatakse ja kasutatakse üha rohkem erinevates valdkondades, alates isiklikust kasutusest kuni kasutamiseni eraettevõtetes ja avalikus halduses. Näotuvastustehnoloogiast ootavad kasu ka õiguskaitseasutused. See pakub lahendusi suhteliselt uutele probleemidele, näiteks uurimised mis hõlmavad suurt hulka tõendeid, aga ka senistele probleemidele, eelkõige kui jälgimis- ja otsinguülesannete täitmiseks napib inimressursse.
2. Suurem huvi näotuvastustehnoloogia vastu tuleneb valdavalt selle tõhususest ja mastaabitavusest. Siit tulenevad ka näotuvastustehnoloogiale ja selle rakendamisele omased puudused, sealhulgas laiemal skaalal. Kuigi ühe nupuvajutusega võib analüüsida tuhandeid isikuandmete kogumeid, võib juba väike algoritmiline diskrimineerimine või väärtuvastus rängalt mõjutada suure hulga isikute käitumist ja igapäevaelu. Isikuandmete, eelkõige biomeetriliste andmete töötlemise ulatus on veel üks näotuvastustehnoloogia põhielement, sest isikuandmete töötlemine kujutab endast sekkumist isikuandmete kaitse põhiõigusesse vastavalt ELi põhiõiguste harta (edaspidi „harta“) artiklile 8.
3. Näotuvastustehnoloogia kohaldamine õiguskaitseasutuste poolt mõjutab tulevikus – ja teatud määral juba praegu – oluliselt üksikisikuid ja inimirühmi, sealhulgas vähemusi. Selle tagajärgedel on märkimisväärne mõju ka meie kogukondlikule elule ning ühiskondlikule ja demokraatlikule poliitilisele stabiilsusele, mis väärtustab kõrgelt pluralismi ja poliitilist opositsiooni. Isikuandmete kaitse õigusel on võtmetähtsus, sageli on ta eeltingimus teiste põhiõiguste tagamiseks. Näotuvastustehnoloogia kohaldamine riivab oluliselt ka teisi põhiõigusi peale isikuandmete kaitse õiguse.
4. Seetõttu peab EDPB oluliseks toetada näotuvastustehnoloogia jätkuvat integreerimist õiguskaitse valdkonnas, mis on reguleeritud õiguskaitse direktiivi¹ ja seda rakendavate siseriiklike õigusaktidega, esitades käesolevad suunised. Suuniste eesmärk on anda asjakohast teavet ELi ja liikmesriikide seadusandjatele, samuti õiguskaitseasutustele ja ametnikele, kes rakendavad ja kasutavad

¹ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.

näotuvastussüsteeme. Suuniste kohaldamisala piirdub näotuvastustehnoloogiaga. Samas töötlevad õiguskaitseasutused biomeetrilisi isikuandmeid ka muul viisil, eeskätt näiteks kaugtuvastusmeetoditega, millega võivad kaasnedä sarnased või täiendavad ohud üksikisikutele, rühmadele ja ühiskonnale. Sõltuvalt konkreetsetest asjaoludest võivad teatud suuniste aspektid olla kasulikud ka taolistel juhtudel. Samuti võivad isikud, kes on teemast huvitatud üldiselt või andmesubjektidena, leida siit olulist teavet, eelkõige seoses andmesubjektide õigustega.

5. Suunised koosnevad põhidokumendist ja kolmest lisast. Põhidokumendis esitatakse tehnoloogia ja kohaldatav õigusraamistik. Et tuvastada põhilisi aspekte, mis võimaldavad liigitada põhiõiguste rikkumise tõsidust konkreetse juhtumi kohaldamisalal, on I lisas esitatud vorm. Õiguskaitseasutused, kes soovivad hankida ja käitada näotuvastussüsteemi, võivad saada II lisast praktilisi juhiseid. Sõltuvalt näotuvastustehnoloogia kohaldamisalast võivad olla asjakohased erinevad kaalutlused. Hüpoteetiliste stsenaariumide ja asjakohaste kaalutluste kogum on esitatud III lisas.

2 TEHNOLOOGIA

2.1 Üks biomeetriline tehnoloogia, kaks erinevat funktsiooni

6. Näotuvastus on tõenäosusel tuginev tehnoloogia, mis võimaldab isikuid nende näo põhjal automaatselt ära tunda, et neid siis autentida või tuvastada.
7. Näotuvastustehnoloogia kuulub laiemasse biomeetrilise tehnoloogia kategooriasse. Biomeetria hõlmab kõiki automatiseeritud protsesse, mida kasutatakse isiku äratundmiseks füüsiliste, füsioloogiliste või käitumuslike tunnuste (sõrmejäljed, iirise struktuur, hääl, kõnnak, veresoonemustrid jne) kvantifitseerimise teel. Need tunnused on määratletud kui „biomeetrilised andmed“, sest need võimaldavad või kinnitavad kõnealuse isiku kordumatut tuvastust.
8. See kehtib inimeste nägude ehk täpsemalt nende tehnilise töötlemise kohta näotuvastusseadmete abil: näo kujutisest (foto või video) ehk biomeetrilisest „proovist“ on võimalik genereerida selle näo eristatavate tunnuste digikujutis (nimetatakse „malliks“).
9. Biomeetriline mall on biomeetrilisest proovist saadud unikaalsete tunnuste digikujutis, mille saab salvestada biomeetrilisse andmebaasi². See mall on eeldatavalt igale inimesele omane ja ainulaadne ning põhimõtteliselt ajas muutumatu³. Tuvastusetapis võrdleb seade seda malli biomeetriliste proovide, näiteks pildil, fotol või videol olevate nägude põhjal varem otse genereeritud või arvutatud teiste mallidega. „Näotuvastus“ on seega kaheetapiline protsess: näokujutise hankimine ja selle teisendamine malliks, millele järgneb näo tuvastamine vastava malli võrdlemisel ühe või mitme teise malliga.
10. Nagu iga biomeetriline protsess, võib ka näotuvastus täita kahte erinevat funktsiooni:
 - Isiku **autentimine**, mille eesmärk on kontrollida, kas isik on see, kes ta väidab end olevat. Sel juhul võrdleb süsteem eelnevalt (nt nutikaardile või biomeetrilisele passile) salvestatud biomeetrilist malli või proovi üheainsa näoga, näiteks kontrollpunkti saabuva isiku näoga, et kontrollida, kas tegemist on ühe ja sama isikuga. See funktsioon põhineb seega kahe malli võrdlemisel. Seda nimetatakse ka üks-ühele **kontrolliks**.

² Näotuvastuse suunised, isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni nr 108 nõuandekomitee, Euroopa Nõukogu, juuni 2021.

³ Sõltub biomeetria tüübist ja andmesubjekti vanusest.

- Isiku **tuvastamine**, mille eesmärk on leida isik isikute rühmast konkreetses piirkonnas, pildil või andmebaasis. Sel juhul peab süsteem töötleva iga jäädvustatud nägu, et luua biomeetriline mall, ja seejärel kontrollima, kas see vastab süsteemis teadaolevale isikule. See funktsioon põhineb seega ühe malli võrdlemisel mallide või proovide andmebaasiga (võrdlusalusel). Seda nimetatakse ka üks-mitmele tuvastamiseks. Näiteks võib süsteem seostada isiku nimekirje (perekonnanimi, eesnimi) näoga, kui võrdlus tehakse perekonna- ja eesnimede ning fotode andmebaasi vahel. See võib hõlmata ka isiku jälgimist rahvahulgas, loomata seost tema kodanikuidentiteediga.

11. Mõlemal juhul põhinevad kasutatud näotuvastustehnoloogiad mallide (võrreldava ja võrdlusalus(t)e) hinnangulisel kokkulangevusel. Sellest aspektist vaadates on tegemist tõenäosuslike tehnoloogiatega: võrdluse põhjal tuletatakse suurem või väiksem tõenäosus, kas isik on tõepoolest see, keda soovitakse autentida või tuvastada; kui tõenäosus ületab süsteemis teatava künnise, mille on määranud süsteemi kasutaja või arendaja, eeldab süsteem, et tegemist on kokkulangevusega.
12. Kuigi need funktsioonid – autentimine ja tuvastamine – on erinevad, on mõlemad seotud tuvastatud või tuvastatava füüsilise isiku biomeetriliste andmete töötlemisega ning kujutavad endast seega isikuandmete, täpsemalt isikuandmete eriliikide töötlemist.
13. Näotuvastus on osa videokujutiste töötlemise tehnikatest. Mõni videokaamera võib filmida teatavas piirkonnas inimesi, eelkõige nende nägusid, kuid neid ei saa sellisel kujul kasutada üksikisikute automaatseks tuvastamiseks. Sama kehtib ka tavaliste fotode kohta: kaamera ei ole näotuvastussüsteem, sest inimeste fotosid tuleb biomeetriliste andmete saamiseks erilisel viisil töödelda.
14. Ka pelk nägude tuvastamine nn nutikaamerate abil ei ole tingimata näotuvastussüsteem. Kuigi digitehnoloogiad tõstatavad küsimusi eetika ja tõhususe kohta, ei saa ebanormaalse käitumise või vägivaldsete sündmuste tuvastamise või nägudel avalduvate emotsioonide või isegi siluettide äratundmise digitehnoloogiaid pidada biomeetrilisteks süsteemideks, mis töötlevad isikuandmete eriliike, kui nende eesmärk ei ole isiku ainulaadne tuvastamine ja asjaomane isikuandmete töötlemine ei hõlma muid isikuandmete eriliike. Need näited ei ole küll näotuvastusest täiesti erinevad ja nende suhtes kohaldatakse isikuandmete kaitse eeskirju.⁴ Pealegi võib seda tüüpi tuvastussüsteemi kasutada koos teiste süsteemidega, mille eesmärk on isiku tuvastamine, ja seda võib seega pidada näotuvastustehnoloogiaks.
15. Erinevalt näiteks videopildistamise ja -töötlemise süsteemidest, mis nõuavad füüsiliste seadmete paigaldamist, on näotuvastus tarkvarafunktsioon, mille saab integreerida olemasolevatesse süsteemidesse (kaamerad, pildiandmebaasid jne). Seda funktsiooni saab seega ühendada või liidestada paljude süsteemidega ja kombineerida muude funktsioonidega. Selline integreerimine olemasolevasse taristusse nõuab erilist tähelepanu, sest sellega kaasnevad ohud, mis tulenevad asjaolust, et näotuvastustehnoloogia võib olla märkamatu ja kergesti varjatud⁵.

2.2 Mitmesugused eesmärgid ja rakendused

16. Väljaspool käesolevate suuniste ja õiguskaitseDirektiivi kohaldamisala võib näotuvastustehnoloogiat kasutada mitmesuguste eesmärkide saavutamiseks, nii kaubanduslikuks kasutuseks kui ka avaliku julgeoleku või õiguskaitsega seotud probleemide lahendamiseks. Seda võib kasutada mitmetes

⁴ ÕiguskaitseDirektiivi artiklit 10 (või isikuandmete kaitse üldmääruse artiklit 9) kohaldatakse siiski süsteemidele, millega liigitatakse isikuid nende biomeetriliste andmete alusel etnilise päritolu, poliitiliste veendumuste, seksuaalse sättumuse või muude isikuandmete eriliikide järgi klastritesse.

⁵ Näiteks kehal kantavad kaamerad, mida praktikas üha enam kasutatakse.

erinevates kontekstides: kasutaja ja teenuse vahelises isiklikus suhtes (juurdepääs rakendusele), juurdepääsuks konkreetsele asukohale (füüsiline filtreerimine) või ilma konkreetse piiranguta avalikus ruumis (reaalajas toimuv näotuvastus). Seda võib kohaldada mis tahes liiki andmesubjektile: teenuse klient, töötaja, lihtsalt pealtvaataja, tagaotsitav või kohtu- või haldusmenetluses osalev isik jne. Mõned kasutusviisid on juba tavalised ja laialt levinud, teised on veel eksperimentaalses või spekulatiivses etapis. Ehkki käesolevates suunistes ei käsitleta kõiki selliseid kasutusviise ja rakendusi, tuleb EDPB meelde, et neid võib rakendada üksnes siis, kui need on kooskõlas kohaldatava õigusraamistikuga, eelkõige isikuandmete kaitse üldmääruse ja asjakohaste riiklike õigusaktidega.⁶ Isegi õiguskaitse direktiivi kontekstis võib – lisaks autentimis- või tuvastusfunktsioonidele – näotuvastustehnoloogiaga töödeldud andmeid täiendavalt töödelda ka muudel eesmärkidel, näiteks kategooriatesse liigitamiseks.

17. Võimalike kasutusviiside ulatust võiks täpsemalt kaaluda sõltuvalt sellest, mil määral inimestel on kontroll oma isikuandmete üle, kas neil on tõhusad vahendid selle kontrolli teostamiseks ja õigus alata sellise tehnoloogia kasutamist, mis tagajärjed neile avalduvad (tuvastamise või mittetuvastamise korral) ja mis oleks teostatava töötlemise ulatus. Näotuvastus, mis põhineb inimese isiklikus seadmes (kiipkaardil, nutitelefoni jne) salvestatud mallil, mida kasutatakse autentimiseks ja rangelt isiklikuks otstarbeks vastava liidese kaudu, ei kujuta endast samasugust ohtu nagu näiteks kasutamine tuvastamise eesmärgil kontrollimata keskkonnas ilma andmesubjektide aktiivse osaluseta, mille korral iga jälgimisalasse siseneva näo malli võrreldakse elanikkonna laialt osalt saadud ja andmebaasi salvestatud mallidega. Nende kahe äärmuse vahele jäävad väga erinevad kasutusala, mis tõstatavad isikuandmete kaitsega seotud küsimusi.
18. Et veelgi selgitada konteksti, milles näotuvastustehnoloogiaid praegu kasutatakse või kasutatakse, peab EDPB asjakohaseks tuua rea näiteid. Allpool esitatud näited on üksnes kirjeldavad ning neid ei tohiks käsitada andmekaitse valdkonna ELi õigustikuga vastavusele antava esialgse hinnanguna.

Näotuvastuse abil autentimise näited

19. Autentimine võib olla kavandatud nii, et kasutajatel on selle üle täielik kontroll, näiteks et võimaldada juurdepääsu teenustele või rakendustele kodus keskkonnas. Nutitefonide omanikud kasutavad seda laialdaselt oma seadme lahtilukustamiseks salasõnapõhise autentimise asemel.
20. Näotuvastuse abil autentimist võib kasutada ka selleks, et kontrollida avalikke või eraõiguslikke kolmandate isikute teenuseid kasutada soovija isikusamasust. Sellised protsessid pakuvad võimalust luua digitaalne identiteet mobiilirakenduse (nutitelefoni, tahvelarvuti jne) abil, mida saab seejärel kasutada juurdepääsuks veebipõhiste haldusteenustele.
21. Lisaks saab näotuvastuse abil autentimisega kontrollida füüsilist juurdepääsu ühele või mitmele eelmääratletud asukohale, näiteks hoonesisepääsudele või konkreetsetele piiripunktidele. Seda funktsiooni rakendatakse näiteks piiriületuse eesmärgil toimivas töötlemises, mille käigus võrreldakse kontrollpunktis isiku nägu tema isikut tõendavas dokumendis (passis või elamisloas) salvestatud näo vastu.

Näotuvastuse abil tuvastamise näited

22. Tuvastamist saab rakendada veelgi mitmekesisemal viisil. Need näited hõlmavad eelkõige järgmisi ELis kasutatavaid, katsetatavaid või kavandatavaid kasutusviise:

⁶ Lisateave on 29. jaanuari 2020. aasta EDPB suunistes 3/2019 isikuandmete töötlemise kohta videoseadmetes.

- otsing fotoandmebaasis, et teha kindlaks tuvastamata isiku (ohvri, kahtlusosaluse jne) isikusamasus;
- isiku liikumise jälgimine avalikus ruumis, kusjuures tema nägu võrreldakse jälgitavas piirkonnas reisivate või reisinud inimeste biomeetriliste mallidega, nt kui unustati pagas või pandi toime kuritegu;
- isiku teekonna ja tema hilisema (teiste isikutega toimunud) suhtluse rekonstrueerimine samade elementide hilisema võrdlemise kaudu, et muu hulgas tuvastada isiku kontaktid;
- tagaotsitavate isikute biomeetriline kaugtuvastus avalikus ruumis, mille käigus võrreldakse kõiki videokaitsekaamerate reaajas salvestatud nägusid julgeolekujõudude andmebaasis olevate nägudega;
- pildil olevate inimeste automaatne tuvastamine, et teha näiteks kindlaks nende suhted konkreetsetes sotsiaalvõrgustikus; pilti võrreldakse nende võrgustiku liikmete mallidega, kes on andnud oma nõusoleku selle funktsiooni kasutamiseks, et saada pakkumisi kontaktide nimelise tuvastuse kohta;
- juurdepääs teenustele: näiteks mõni sularahaautomaat tuvastab kliente, võrreldes kaamera ga salvestatud näokujutist panga näokujutiste andmebaasiga;
- reisija teekonna jälgimine teatud reisie tapis, mille käigus võrreldakse kõigi teatud reisie tappidel (pagasi äraandmispunktid, pardalemineku väravad jne) asuvates väravates registreeruvate isikute reaajas arvutatud näomalle eelnevalt süsteemis registreeritud isikute mallidega.

23. Lisaks näotuvastustehnoloogia kasutamisele õiguskaitse valdkonnas nõuavad kirjeldatud erinevad rakendused kindlasti põhjalikku arutelu ja poliitilist lähenemisviisi, et tagada järjepidevus ja vastavus ELi andmekaitse raamistikuga.

2.3 Usaldusväarsus, täpsus ja ohud andmesubjektidele

24. Nagu iga tehnoloogiaga, võib tekkida probleeme ka näotuvastuse rakendamisel, eelkõige seoses selle usaldusväarsuse ja tõhususega autentimisel või tuvastamisel, samuti näotuvastustehnoloogia lähteandmete ja töötlustulemuste üldise kvaliteedi ja täpsusega.
25. Need tehnoloogilised probleemid tekitavad puudutatud andmesubjektidele erilisi riske, mis on õiguskaitse valdkonnas veelgi olulisemad või tõsisemad, arvestades andmesubjektidele avalduvaid õiguslikke või muid sarnaseid, neid oluliselt mõjutavaid tagajärgi. Sellega seoses on sobiv rõhutada, et näotuvastustehnoloogia kasutamine tagantjärele ei ole iseenesest turvalisem, sest üksikisikuid võib jälgida eri ajahetkedel ja erinevates kohtades. Seega kaasnevad ka tagantjärele kasutamise ga konkreetsed riskid, mida tuleb juhtumipõhiselt hinnata.⁷
26. Euroopa Liidu Põhiõiguste Amet märkis oma 2019. aasta aruandes, et „näotuvastustarkvara vajaliku täpsuse taseme kindlaksmääramine on keeruline: täpsust saab hinnata paljudel erinevatel viisidel, sõltuvalt ka ülesandest, eesmärgist ja kasutuskontekstist. Kui seda tehnoloogiat kohaldatakse kohtades, mida külastavad miljonid inimesed – näiteks raudteejaamades või lennujaamades –, tähendab ka suhteliselt väike eksimuste protsent (nt 0,01%)⁸, et sajad inimesed on valesti märgistatud. Lisaks võib teatud isikute kategooriates olla vale kokkulangevuse tõenäosus suurem kui teistes, nagu on kirjeldatud 3 jaos. Veamäärade arvutamiseks ja tõlgendamiseks on erinevaid meetodeid, seega

⁷ Vt III lisas esitatud näited.

⁸ See täpsusmäär tuleneb tsiteeritud aruandest ja on palju kõrgem kui näotuvastustehnoloogiarakenduste algoritmide hetketulemuslikkus.

tuleb olla ettevaatlik. Samuti on täpsuse ja vigadega seoses oluline küsida, kui kergesti saab süsteemi petta näiteks võltsitud näokujutistega (*spoofing* ehk teesklus), eriti õiguskaitse seisukohalt.⁹

27. Sellega seoses peab EDPB oluliseks meelde tuletada, et näotuvastustehnoloogia, olenemata sellest, kas seda kasutatakse autentimiseks või identifitseerimiseks, ei anna lõplikku tulemust, vaid tugineb tõenäosusele, et kaks nägu või näokujutist vastavad samale isikule.¹⁰ See tulemus on veelgi ebaselgem, kui näotuvastussüsteemi sisestatava biomeetrilise malli kvaliteet on halb. Sisendpildi hägusus, kaamera väike resolutsioon, liikumine ja vähene valgus võivad anda halva kvaliteediga tulemuse. Muud tulemusi oluliselt mõjutavad aspektid on näotuvastustehnoloogia lai levik ja teesklus, nt kui kurjategijad püüavad kas vältida kaamerasse sattumist või näotuvastustehnoloogiat petta. Arvukad uuringud on samuti näidanud, et algoritmilise töötlemise statistilised tulemused võivad olla kallutatud, eelkõige tulenevalt lähteandmete kvaliteedist ja algoritmide õpetamiseks kasutatavatest andmebaasidest või muudest teguritest, nt asukoha valik. Samamoodi tuleks rõhutada näotuvastustehnoloogia mõju muudele põhiõigustele, näiteks era- ja perekonnavabadusele, sõna- ja teabevabadusele, kogunemis- ja ühinemisvabadusele jne.
28. Seetõttu on oluline, et näotuvastustehnoloogia usaldusväärsust ja täpsust võetaks arvesse kui kriteeriume, mille alusel hinnatakse vastavust õiguskaitse direktiivi artiklis 4 sätestatud andmekaitsepõhimõtetele, eelkõige seoses õigluse ja täpsusega.
29. Märkides, et kvaliteetsed andmed on kvaliteetsete algoritmide jaoks hädavajalikud, rõhutab EDPB ühtlasi, et vastutavad töötlejad peavad oma aruandekohustuse raames korrapäraselt ja süstemaatiliselt hindama algoritmilist töötlemist, et tagada eelkõige sellise isikuandmete töötlemise tulemuste täpsus, õiglus ja usaldusväärsus. Isikuandmeid, mida kasutatakse näotuvastussüsteemide hindamiseks, õpetamiseks ja edasiarendamiseks, tohib töödelda üksnes siis, kui on olemas piisav õiguslik alus, ja kooskõlas ühiste andmekaitsepõhimõtetega.

3 KOHALDATAV ÕIGUSRAAMISTIK

30. Näotuvastustehnoloogiate kasutamine on lahutamatu seotud isikuandmete, sealhulgas andmete eriliikide töötlemisega. Peale selle mõjutab see otseselt või kaudselt mitmeid põhiõigusi, mis on sätestatud ELi põhiõiguste hartas. See on eriti oluline õiguskaitse ja kriminaalõiguse valdkonnas. Seetõttu tuleks näotuvastustehnoloogiat kasutada ranges kooskõlas kohaldatava õigusraamistikuga.
31. Allpool esitatud teavet tuleks näotuvastustehnoloogia valdkonna tulevaste seadusandlike ja haldusmeetmete hindamisel ning olemasolevate õigusaktide rakendamisel juhtumipõhiselt arvesse võtta. Vastavate nõuete asjakohasus sõltub konkreetsetest asjaoludest. Kuna kõiki tulevasi asjaolusid ei ole võimalik ette näha, on see loetelu üksnes toetav ja mitteammendav.

3.1 Üldine õigusraamistik – ELi põhiõiguste harta ja Euroopa inimõiguste ja põhivabaduste kaitse konventsioon

⁹ Näotuvastustehnoloogia: põhiõiguste kaalutlused õiguskaitse kontekstis, Euroopa Liidu Põhiõiguste Amet, 21.11.2019.

¹⁰ Seda tõenäosust nimetatakse „usaldusväärsuse skooriks“.

3.1.1 Harta kohaldatavus

32. ELi põhiõiguste harta (edaspidi „harta“) on ette nähtud liidu institutsioonidele, organitele ja asutustele ning liikmesriikidele liidu õiguse kohaldamise korral.
33. Õiguskaitse eesmärgil biomeetriliste andmete töötlemise reguleerimine vastavalt õiguskaitse direktiivi artikli 1 lõikele 1 tõstatatakse paratamatult küsimuse, kas järgitakse põhiõigusi, eelkõige harta artiklis 7 sätestatud eraelu ja sõnumite puutumatust ning harta artiklis 8 sätestatud isikuandmete kaitse õigust.
34. Füüsiliste isikute, sealhulgas nende nägude videokaadrite kogumine ja analüüsimine tähendab isikuandmete töötlemist. Kujutise tehniline töötlemine hõlmab ka biomeetrilisi andmeid. Füüsilise isiku näo andmete tehniline töötlemine aja ja koha kontekstis võimaldab teha järeldusi puudutatud isikute eraelu kohta. Need järeldused võivad viidata rassilisele või etnilisele päritolule, tervisele, usule, igapäevastele harjumustele, alalisele või ajutisele elukohale, igapäevastele või muudele liikumistele, tegevusaladele, nende isikute ühiskondlikele suhetele ja ringkondadele, kellega nad seostuvad. Näotuvastustehnoloogia kohaldamisel avalikustatud teabe suur hulk näitab selgelt võimalikku mõju harta artiklis 8 sätestatud isikuandmete kaitse õigusele, aga ka harta artiklis 7 sätestatud era- ja perekonnaelu austamise õigusele.
35. Sellises olukorras ei ole mõeldamatu, et asjaomaste biomeetriliste (näo)andmete kogumine, analüüsimine ja edasine töötlemine võiks mõjutada inimeste vaba tegutsemist, isegi kui see tegutsemine toimub vaba ja avatud ühiskonna lubatud piirides. Samuti võib see suuresti mõjutada nende põhiõiguste, näiteks harta artiklites 1, 10, 11 ja 12 sätestatud mõtte-, südametunnistuse- ja usuvabaduse, rahumeelse kogunemise vabaduse ja ühinemise vabaduse õiguste teostamist. Sellise töötlemisega kaasnevad ka muud riskid, näiteks asjaomaste asutuste kogutud isikuandmete kuritarvitamise risk, mis võib tuleneda isikuandmetele ebaseaduslikust juurdepääsust ja nende kasutamisest, turvanõuete rikkumistest jne. Riskid sõltuvad sageli töötlemisest ja selle asjaoludest, näiteks politsei ametnike või teiste volitatud isikute poolse ebaseadusliku juurdepääsu ja andmete kasutamise risk. Mõned riskid tulenevad aga biomeetriliste andmete ainulaadsest olemusest. Erinevalt aadressist või telefoninumbrist ei saa andmesubjekt muuta oma ainulaadseid omadusi, nagu nägu või silmapiirid. Biomeetrilistele andmetele loata juurdepääs või nende juhuslik avaldamine võib ohustada andmete kasutamist parooli või krüptograafilise võtmega või seda võidakse kasutada edasiseks loata jälgimistegevuseks, mis kahjustab andmesubjekti.

3.1.2 Sekkumine hartas sätestatud õigustesse

36. Biomeetriliste andmete töötlemine on igas olukorras iseenesest tõsine sekkumine. See ei sõltu tulemusest, näiteks positiivsest kokkulangevusest. Töötlemine on sekkumine isegi siis, kui biomeetriline mall kustutatakse kohe pärast seda, kui võrdlemine politsei andmebaasiga ei anna päringutabamust.
37. Andmesubjektide põhiõigustesse sekkumine võib tuleneda õigusaktist, mille eesmärk või tagajärg on vastava põhiõiguse piiramine¹¹. See võib tuleneda ka riigiasutuse sama eesmärgi või mõjuga toimingust või isegi sellise eraõigusliku üksuse toimingust, kellele on seadusega antud avaliku võimu teostamise volitus.

¹¹ Euroopa Liidu Kohtu otsus kohtuasjas C-219/91 – Ter Voort, RoC 1992 I-05485, punkt 36f; Euroopa Liidu Kohtu otsus kohtuasjas C-200/96 – Metronome, RoC 1998 I-1953, punkt 28.

38. Seadusandlik meede, mis on isikuandmete töötlemise õiguslik alus, sekkub otseselt harta artiklitega 7 ja 8 tagatud õigustesse¹².
39. Biomeetriliste andmete ja eelkõige näotuvastustehnoloogia kasutamine mõjutab paljudel juhtudel ka õigust inimväärikusele, mis on tagatud harta artikliga 1. Inimväärikus nõuab, et üksikisikuid ei käsitataks pelgalt objektidena. Näotuvastustehnoloogia arvutab välja näojooned, olemuslikud ja väga isiklikud tunnused, ning muundab need masinloetavale kujule, et kasutada seda nn isiku registreerimismärgi või ID-kaardina, objektisades seega näo.
40. Selline töötlemine võib sekkuda ka muudesse põhiõigustesse, näiteks harta artiklitest 10, 11 ja 12 tulenevatesse õigustesse, sest õiguskaitseasutuste videovalvele on mõeldud või sellest tuleneb heidutav mõju.
41. Lisaks tuleks hoolikalt kaaluda ka võimalikke riske, mis tulenevad näotuvastustehnoloogiate kasutamisest õiguskaitseorganite poolt seoses harta artiklites 47 ja 48 sätestatud õiglase kohtumenetluse ja süütuse presumptsiooniga. Näotuvastustehnoloogia kohaldamise tulemus, näiteks kokkulangevus, võib lisaks isiku edasisele politseijärelevalvele olla ka otsustav tõend kohtumenetluses. Näotuvastustehnoloogia puudused, näiteks võimalik kallutus, diskrimineerimine või valetuvastus („valepositiivsed juhtumid“), võivad seega tekitada raskeid tagajärgi ka kriminaalmenetluses. Lisaks võidakse tõendite hindamisel eelistada näotuvastustehnoloogia kohaldamise tulemust, isegi kui esinevad vasturääkivad tõendid (nn kalduvus eelistada automatiseerimist).

3.1.3 Sekkumise õigustus

42. Harta artikli 52 lõike 1 kohaselt peavad põhiõiguste ja -vabaduste kasutamise piirangud olema sätestatud seadusega ning olema kooskõlas nende õiguste ja vabaduste olemusega. Proportsionaalsuse põhimõtte kohaselt võib piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

3.1.3.1 Sätestatud seaduses

43. Harta artikli 52 lõikes 1 on sätestatud konkreetse õigusliku aluse nõue. Õiguslik alus peab olema piisavalt selge, et anda kodanikele adekvaatset teavet tingimuste ja asjaolude kohta, mille korral ametiasutustel on volitus kasutada mis tahes andmete kogumise ja salajase jälgimise meetmeid¹³. See peab piisava selgusega näitama ametiasutustele antud kaalutusõiguse kasutamise ulatust ja viisi, et tagada üksikisikutele demokraatlikus ühiskonnas õigusriigi põhimõttele vastav minimaalne kaitsetase¹⁴. Lisaks nõuab seaduslikkuse põhimõtte piisavaid kaitsemeetmeid, et tagada üksikisikule eelkõige harta artiklis 8 sätestatud õiguse järgimist. Samu põhimõtteid kohaldatakse ka isikuandmete töötlemisel näotuvastussüsteemide hindamise, õpetamise ja edasiarendamise eesmärgil.
44. Arvestades, et füüsilise isiku kordumatu tuvastamise eesmärgil töödeldavad biomeetrilised andmed on õiguskaitse direktiivi artiklis 10 loetletud andmete eriliigid, nõuaksid näotuvastustehnoloogia erinevad rakendused enamikul juhtudel eriõigusakti, milles kirjeldatakse täpselt rakendust ja selle kasutustingimusi. See hõlmab eelkõige konkreetseid kuriteoliike ja vajadusel nende kuritegude asjakohast raskusastet, et muu hulgas tõhusalt välistada pisikuriteod.¹⁵

¹² Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 36; Euroopa Liidu Kohtu otsus kohtuasjas C-291/12, punkt 23 jj.

¹³ Euroopa Inimõiguste Kohtu otsus kohtuasjas Shimovolos vs. Venemaa, punkt 68; Vukota-Bojić vs. Šveits.

¹⁴ Euroopa Inimõiguste Kohtu otsus kohtuasjas Piechowicz vs. Poola, punkt 212.

¹⁵ Vt nt Euroopa Liidu Kohtu otsused kohtuasjades C-817/19, Ligue des droits humains, punkt 151f; C-207/16, Ministerio Fiscal, punkt 56.

3.1.3.2 Harta artiklites 7 ja 8 sätestatud era- ja perekonnaelu austamise ning isikuandmete kaitse põhiõiguste olemus

45. Erinevatest olukordadest lähtuvad põhiõiguste piirangud peavad siiski tagama konkreetse õiguse olemuse austamise. Olemus viitab asjaomase põhiõiguse põhisisele¹⁶. Inimväärikust tuleb austada ka siis, kui õigust piiratakse¹⁷.
46. Puutumatu põhisise võimaliku rikkumise tunnused on järgmised:
- Säte, millega kehtestatakse piirangud olenemata isiku individuaalsest käitumisest või erandlikest asjaoludest¹⁸.
 - Kohtusse pöördumine ei ole võimalik või on takistatud¹⁹.
 - Enne õiguse ranget piiramist ei võeta puudutatud isiku asjaolusid arvesse²⁰.
 - Harta artiklites 7 ja 8 sätestatud õigusi silmas pidades: Lisaks side metaandmete ulatuslikule kogumisele võib elektroonilise side sisu kohta teadmiste omandamine rikkuda nende õiguste olemust²¹.
 - Harta artiklites 7, 8 ja 11 sätestatud õigusi silmas pidades: Õigusnormid, millega nõutakse, et avalikele veebipõhiste sideteenustele juurdepääsu pakkujad ja veebimajutusteenuse pakkujad säilitaksid üldiselt ja vahet tegemata muu hulgas nende teenustega seotud isikuandmeid²².
 - Harta artiklis 8 sätestatud õigusi silmas pidades: Andmekaitse ja andmeturbe aluspõhimõtete puudumine võib samuti rikkuda õiguse põhisise²³.

3.1.3.3 Õiguspärane eesmärk

47. Nagu juba selgitatud punktis 3.1.3., peavad põhiõiguste piirangud vastama Euroopa Liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või vastama vajadusele kaitsta teiste isikute õigusi ja vabadusi.
48. Liit tunnustab nii ELi lepingu artiklis 3 nimetatud eesmärges kui ka muid huve, mida kaitsevad aluslepingute konkreetsed sätted²⁴, st – muu hulgas – vabadusel, turvalisusel ja õigusel rajanev ala, kuritegevuse ennetamine ja selle vastu võitlemine. Oma suhetes muu maailmaga peaks liit aitama kaasa rahu ja julgeoleku tagamisele ning inimõiguste kaitsele.
49. Vajadus kaitsta teiste isikute õigusi ja vabadusi viitab isikute õigustele, mis on kaitstud Euroopa Liidu või selle liikmesriikide õigusega. Hindamise eesmärk peab olema ühitada vastavate õiguste kaitse nõuded ja tagada nende vahel õiglane tasakaal²⁵.

3.1.3.4 Vajalikkuse ja proportsionaalsuse kontroll

50. Kui tegemist on põhiõigustesse sekkumisega, võib siseriikliku ja liidu seadusandja kaalutusõiguse ulatus osutada piiratuks. See sõltub mitmest tegurist, sealhulgas asjaomasest valdkonnast, hartaga tagatud konkreetse õiguse olemusest, sekkumise laadist ja raskusastmest ning sekkumise

¹⁶ Euroopa Liidu Kohtu otsus kohtuasjas C-279/09, RoC 2010 I-13849, punkt 60.

¹⁷ Selgitused põhiõiguste harta kohta, I jaotis, selgitus artikli 1 kohta, ELT C 303, 14.12.2007, lk 17–35.

¹⁸ Euroopa Liidu Kohtu otsus kohtuasjas C-601/15, punkt 52.

¹⁹ Euroopa Liidu Kohtu otsus kohtuasjas C-400/10, RoC 2010 I-08965, punkt 55.

²⁰ Euroopa Liidu Kohtu otsus kohtuasjas C-408/03, RoC 2006 I-02647, punkt 68.

²¹ Euroopa Liidu Kohtu otsus kohtuasjas C-203/15, Tele2 Sverige, punkt 101, viitega otsusele kohtuasjas C-293/12 ja C-594/12, punkt 39.

²² Euroopa Liidu Kohtu otsus kohtuasjas C-512/18, La Quadrature du Net, punkt 209 jj.

²³ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 40.

²⁴ Selgitused põhiõiguste harta kohta, I jaotis, selgitus artikli 52 kohta, ELT C 303, 14.12.2007, lk 17–35.

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

eesmärgist²⁶. Seadusandlikud meetmed peavad olema asjaomaste õigusaktidega taotletavate õiguspäraste eesmärkide saavutamiseks sobivad. Samuti ei tohi meede ületada piire, mis on nende eesmärkide saavutamiseks asjakohased ja vajalikud²⁷. Üldise huvi eesmärk – kui tahes oluline – ei õigusta iseenesest põhiõiguse piiramist²⁸.

51. Euroopa Liidu Kohtu väljakujunenud praktika kohaselt tuleb isikuandmete kaitsega seotud erandeid ja piiranguid kohaldades piirduda ainult rangelt vajalikuga²⁹. See tähendab ühtlasi, et eesmärgi saavutamiseks ei ole vähem sekkuvaid vahendeid. Võimalikud alternatiivid, näiteks – sõltuvalt eesmärgist – lisapersonal, sagedasemad politseipatrullid või täiendav tänavavalgustus, tuleb hoolikalt välja selgitada ja neid tuleb hinnata. Seadusandlikud meetmed peaksid olema diferentseeritud ja suunatud isikutele, kes võiksid olla sihtrühmaks, võttes arvesse eesmärki, nt võitlust raske kuritegevuse vastu. Kui meede hõlmab üldiselt kõiki isikuid ilma eristamise, piiramise või erandite kohaldamiseeta, süvendab see sekkumist³⁰. Sekkumist süvendab ka see, kui andmetöötlus hõlmab olulist osa elanikkonnast³¹.
52. Isikuandmete kaitse, mis tuleneb harta artikli 8 lõikes 1 sätestatud sõnaselgest kohustusest, on eriti oluline seoses harta artiklis 7 sätestatud õigusega era- ja perekonnaelu austamisele³². Õigusnormid peavad sätestama kõnealuse meetme ulatuse ja kohaldamise selged ja täpsed eeskirjad ning kehtestama kaitsemeetmed, et isikutel, kelle andmeid töödeldi, oleksid piisavad tagatised, et tõhusalt kaitsta oma isikuandmeid kuritarvitamise ohu ning mis tahes ebaseadusliku juurdepääsu või kasutamise eest³³. Selliste kaitsemeetmete vajadus on veel suurem, kui isikuandmeid töödeldakse automaatselt ja esineb märkimisväärne oht, et andmetele pääsetakse juurde ebaseaduslikult³⁴. Lisaks võib kaitsemeetmena olla kasu näotuvastustehnoloogia kasutamise sisesest või välisest, nt kohtulikust lubamisest, ning see võib osutuda vajalikuks teatavatel raske sekkumise juhtudel.³⁵
53. Kehtestatud eeskirju tuleb kohandada konkreetsele olukorrale, näiteks töödeldavate andmete kogusele, andmete olemusele³⁶ ja andmetele ebaseadusliku juurdepääsu riskile. See nõuab eeskirju,

²⁶ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 47, koos järgmiste allikatega: vt analoogia alusel Euroopa inimõiguste konventsiooni artikkel 8, Euroopa Inimõiguste Kohtu otsus kohtuasjas H.R., S. and Marper vs. Ühendkuningriik [GC], 30562/04 ja 30566/04, punkt 102, ECHR 2008-V.

²⁷ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 46 koos järgmiste allikatega: kohtuasi C-343/09, Afton Chemical, EU:C:2010:419, punkt 45; Volker und Markus Schecke and Eifert, EU:C:2010:662, punkt 74; kohtuasjad C-581/10 ja C-629/10 Nelson jt, EU:C:2012:657, punkt 71; kohtuasi C-283/11, Sky Österreich EU:C:2013:28, punkt 50, ja kohtuasi C-101/12 Schaible, EU:C:2013:661, punkt 29.

²⁸ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 51.

²⁹ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 52, koos järgmiste allikatega: kohtuasi C-473/12, IPI EU:C:2013:715, punkt 39 ja viidatud kohtupraktika.

³⁰ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 57.

³¹ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 56.

³² Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 53.

³³ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 54, koos järgmiste allikatega: vt analoogia alusel seoses Euroopa inimõiguste konventsiooni artikliga 8, Euroopa Inimõiguste Kohtu otsus kohtuasjas Liberty jt vs. Ühendkuningriik, 1.7.2008, 58243/00, punktid 62 ja 63; Rotaru vs. Rumeenia, punktid 57–59, ja S. ja Marper vs. Ühendkuningriik, punkt 99.

³⁴ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 55, koos järgmiste allikatega: vt analoogia põhjal seoses Euroopa inimõiguste konventsiooni artikliga 8, S. ja Marper vs. Ühendkuningriik, punkt 103, ja M. K. vs. Prantsusmaa, 18.4.2013, 19522/09, punkt 35.

³⁵ Euroopa Inimõiguste Kohtu otsus kohtuasjas Szabó ja Vissy vs. Ungari, punktid 73–77.

³⁶ Vt ka tugevdatud nõuded tehniliste ja korralduslike meetmete kohta andmete eriliikide töötlemisel, õiguskaitseDirektiivi artikli 29 lõige 1.

mis eeskätt reguleeriksid kõnealuste andmete kaitset ja turvalisust selgel ja rangel viisil, et tagada nende terviklikkus ja konfidentsiaalsus³⁷.

54. Seoses vastutava töötleja ja volitatud töötleja suhtega ei tohiks volitatud töötlejatel olla lubatud võtta isikuandmetele kohaldatava turvalisuse taseme kindlaksmääramisel arvesse ainult majanduslikke kaalutlusi; see võib ohustada piisavat kõrget kaitsetaset³⁸.
55. Õigusaktis tuleb sätestada sisulised ja menetlustingimused ning objektiivsed kriteeriumid, mille alusel määratakse kindlaks pädevate asutuste andmetele juurdepääsu ja edasise kasutamise piirangud. Ennetamise, avastamise või kriminaalvastutusele võtmise eesmärgil tuleks asjaomaseid kuritegusid pidada piisavalt raskeks, et õigustada näiteks harta artiklites 7 ja 8 sätestatud põhiõigustesse sekkumise ulatust ja raskusastet³⁹.
56. Andmeid tuleb töödelda viisil, mis tagab ELi andmekaitse-eeskirjade kohaldatavuse ja mõju, eelkõige seoses harta artikli 8 sättega, mille kohaselt kaitse- ja turvanõuete täitmist kontrollib sõltumatu asutus. Geograafiline asukoht, kus töötlemine toimub, võib olla sellises olukorras asjakohane⁴⁰.
57. Isikuandmete töötlemise eri etappidega seoses tuleks eristada andmeliike lähtuvalt nende võimalikust kasulikkusest eesmärgi saavutamisel või lähtuvalt puudutatud isikutest⁴¹. Töötlemise tingimuste, näiteks säilitusperioodi kindlaksmääramine, peab põhinema objektiivsetel kriteeriumitel, et tagada, et sekkumine piirduks üksnes vältimatult vajalikuga⁴².
58. Vastavalt juhtumile tuleb vajaduse ja proportsionaalsuse hindamisel kindlaks teha ja kaaluda kõiki tagajärgi, mis kuuluvad teiste põhiõiguste, näiteks harta artiklis 1 sätestatud inimväärikuse, harta artiklis 10 sätestatud mõtte-, südametunnistuse- ja usuvabaduse, harta artiklis 11 sätestatud sõnavabaduse ning harta artiklis 12 sätestatud kogunemis- ja ühinemisvabaduse kohaldamisalasse.
59. Samuti tuleb pidada tõsiseks probleemiks seda, et andmete süstemaatiline töötlemine ilma andmesubjektide teadmata loob tõenäoliselt üldise pideva jälgimise ettekujutuse⁴³. Sel võib olla heidutav mõju mõnele või kõigile asjaomastele põhiõigustele.
60. Et hõlbustada ja rakendada õiguskaitse valdkonnas näotuvastusega seotud seadusandlike meetmete vajalikkuse ja proportsionaalsuse hindamist, võiksid liikmesriikide ja liidu seadusandjad kasutada olemasolevaid praktilisi vahendeid, mis on spetsiaalselt selle ülesande täitmiseks välja töötatud. Eelkõige võiks kasutada Euroopa Andmekaitseinspektori väljatöötatud vajalikkuse ja proportsionaalsuse vahendikomplekti⁴⁴.

3.1.3.5 Harta artikli 52 lõige 3 ja artikkel 53 (kaitse tase, ka seoses Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga)

61. Vastavalt harta artikli 52 lõikele 3 ja artiklile 53 peavad nendel harta õigustel, mis vastavad Euroopa inimõiguste kaitse konventsiooniga tagatud õigustele, olema sama tähendus ja ulatus, mis on

³⁷ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 66.

³⁸ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 67.

³⁹ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punktid 60 ja 61.

⁴⁰ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 68.

⁴¹ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 63.

⁴² Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 64.

⁴³ Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 37.

⁴⁴ Euroopa Andmekaitseinspektor: „Isikuandmete kaitse põhiõigust piiravate meetmete vajalikkuse hindamine: vahendikomplekt“ (11.4.2017); Euroopa andmekaitseinspektor: „Euroopa andmekaitseinspektori suunised eraelu puutumatuse ja isikuandmete kaitse põhiõigusi piiravate meetmete proportsionaalsuse hindamise kohta“ (19. 12.2019).

sätestatud Euroopa inimõiguste konventsioonis. Kui harta artiklile 7 võib leida vaste Euroopa inimõiguste konventsioonist, siis harta artikli 8 puhul ei ole see nii⁴⁵. Harta artikli 52 lõige 3 ei takista liidu õigusel pakkuda ulatuslikumat kaitset. Kuna Euroopa inimõiguste konventsioon ei ole õigusakt, mis on ametlikult kaasatud ELi õigusesse, tuleb ELi õigusakte kohaldada harta põhiõigusi silmas pidades⁴⁶.

62. Euroopa inimõiguste konventsiooni artikli 8 kohaselt ei tohi avaliku võimu kandja sekkuda era- ja perekonnaelu austamise õiguse kasutamisesse, välja arvatud juhul, kui see on kooskõlas seadusega ja on demokraatlikus ühiskonnas vajalik riigi julgeoleku, avaliku julgeoleku või riigi majandusliku heaolu huvides, korrariikumiste või kuritegevuse ennetamiseks, tervise või kõlbluse kaitseks või teiste isikute õiguste ja vabaduste kaitseks.
63. Euroopa inimõiguste konventsioonis on sätestatud ka standardid seoses sellega, kuidas piiranguid kehtestada. Üks põhioõue lisaks õigusriigi põhimõttele on ettenähtavus. Ettenähtavuse nõude täitmiseks peab riiklik õigus olema piisavalt selge, et anda kodanikele piisavalt teavet, mis asjaoludel ja tingimustel on ametiasutustel õigus selliseid meetmeid kasutada⁴⁷. Seda nõuet tunnustavad Euroopa Liidu Kohus ja ELi andmekaitsealased õigusaktid (vt punkt 3.2.1.1).
64. ⁴⁸ Euroopa inimõiguste konventsiooni artiklis 8 sätestatud õiguste täpsustamiseks tuleb täielikult järgida ka isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni⁴⁹. Tuleb siiski arvestada, et need sätted esindavad liidu kehtivat õigust silmas pidades üksnes miinimumstandartid.

3.2 Konkreetne õigusraamistik - õiguskaitseDirektiiv

65. ÕiguskaitseDirektiivis on sätestatud näotuvastustehnoloogia kasutamiseks teatud raamistik. Kõigepealt määratletakse õiguskaitseDirektiivi artikli 3 lõikes 13 mõistet „biomeetrilised andmed“⁵⁰. Üksikasjalik teave vt eespool punktis 2.1. Teiseks selgitatakse artikli 8 lõikes 2, et seaduslikkuse tagamiseks peab mis tahes töötlemine – lisaks sellele, et see on vajalik õiguskaitseDirektiivi artiklis 1 lõikes 1 sätestatud eesmärkide saavutamiseks – olema reguleeritud siseriikliku õigusega, milles täpsustatakse vähemalt töötlemise üldised eesmärgid, töödeldavad isikuandmed ja töötlemise konkreetsed eesmärgid. Muud olulised sätted mis on seotud biomeetriliste andmetega on õiguskaitseDirektiivi artiklid 10 ja 11. Artiklit 10 tuleb lugeda koostoimes õiguskaitseDirektiivi artikliga 8⁵¹. Alati tuleks järgida õiguskaitseDirektiivi artiklis 4 sätestatud isikuandmete töötlemise põhimõtteid ning nendest tuleks juhendada ka võimalikel näotuvastustehnoloogiat kasutava biomeetrilise töötlemise hindamisel.

⁴⁵ Euroopa Liidu Kohtu otsus kohtuasjas C-203/15, Tele2 Sverige, punkt 129.

⁴⁶ Euroopa Liidu Kohtu otsus kohtuasjas C-311/18, punkt 99.

⁴⁷ Euroopa Inimõiguste Kohtu otsus CASE OF COPLAND vs. ÜHENDKUNINGRIIK, 3.4.2007, taotlus nr 62617/00, punkt 46.

⁴⁸ ETS nr 108.

⁵⁰ ÕiguskaitseDirektiivi artikli 3 lõige 13: „biomeetrilised andmed“ – konkreetse tehnilise töötlemise abil saadavad isikuandmed füüsilise isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutus ja sõrmejälgede andmed.

⁵¹ WP258, arvamus õiguskaitseDirektiivi (EL 2016/680) teatud põhiküsimuste kohta, lk 7.

3.2.1 Andmete eriliikide töötlemine õiguskaitse eesmärgil

66. Vastavalt õiguskaitse direktiivi artiklile 10 on andmete eriliikide, näiteks biomeetriliste andmete töötlemine lubatud üksnes juhul, kui see on rangelt vajalik ja kui andmesubjekti õiguste ja vabaduste kaitseks on kehtestatud asjakohased kaitsemeetmed. Lisaks on see lubatud ainult juhul, kui see on lubatud liidu või liikmesriigi õigusega, et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve või kui selline töötlemine on seotud andmetega, mille andmesubjekt on ilmselgelt avalikustanud. See üldine klausel rõhutab andmete eriliikide töötlemise tundlikkust.

3.2.1.1 Lubatud liidu või liikmesriigi õigusega

67. Seoses vajaliku seadusandliku meetme liigiga on õiguskaitse direktiivi põhjenduses 33 sätestatud, et „[k]ui käesolevas direktiivis osutatakse liikmesriigi õigusele, õiguslikule alusele või seadusandlikule meetmele, ei pea selleks tingimata olema parlamendi poolt vastu võetud seadusandlik akt, ilma et see piiraks asjaomase liikmesriigi põhiseaduslikust korrast tulenevate nõuete kohaldamist“.⁵²
68. Harta artikli 52 lõike 1 kohaselt tohib hartaga tunnustatud õiguste ja vabaduste teostamist piirata „ainult seadusega“. See kordab Euroopa inimõiguste konventsiooni artikli 8 lõikes 2 kasutatud väljendit „kooskõlas seadusega“, mis tähendab mitte ainult siseriikliku õiguse järgimist, vaid on seotud ka selle õiguse kvaliteediga, nõudes selle kooskõla õigusriigi põhimõttega, kuid piiramata seejuures õigusakti olemust.
69. Õiguskaitse direktiivi põhjenduses 33 on lisaks öeldud, et „[s]elline liikmesriigi õigus, õiguslik alus või seadusandlik meede peaks siiski olema selge ja täpne ning selle kohaldamine ettenähtav nendele, kelle suhtes seda kohaldatakse, nagu seda nõuab Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktika. Käesoleva direktiivi kohaldamisalasse kuuluvat isikuandmete töötlemist reguleerivas liikmesriigi õiguses tuleks kindlaks määrata vähemalt isikuandmete töötlemise üldeesmärgid, töödeldavad isikuandmed, töötlemise konkreetsed eesmärgid ning isikuandmete tervikluse ja konfidentsiaalsuse tagamise menetlused ja isikuandmete hävitamist käsitlevad menetlused.“
70. Eelkõige peab siseriiklik õigus olema oma sõnastuses piisavalt selge, et anda kodanikele piisavalt teavet, mis asjaoludel ja tingimustel on vastutavatel töötlejatel õigus selliseid meetmeid kasutada. See hõlmab töötlemise võimalikke eeltingimusi, näiteks konkreetseid tõendiliike, samuti vajadust kohtu- või sisemise loa järele. Vastav õigusakt võib olla tehnoloogianeutraalne, kui näotuvastustehnoloogia abil isikuandmete töötlemise konkreetseid ohtusid ja eriomadusi on piisavalt käsitletud. Kooskõlas õiguskaitse direktiiviga ning Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu kohtupraktikaga on tõepoolest oluline, et seadusandlikud meetmed, mille eesmärk on luua näotuvastusmeetmete õiguslik alus, oleksid andmesubjektide jaoks ettenähtavad.
71. Seadusandlikule meetmele ei saa tugineda kui õigusaktina, millega antakse luba biomeetriliste andmete töötlemiseks näotuvastustehnoloogia abil õiguskaitse eesmärgil, kui see meede võtab pelgalt üle õiguskaitse direktiivi artikli 10 üldise sätte.
72. Lisaks biomeetrilistele andmetele reguleerib õiguskaitse direktiivi artikkel 10 ka muude andmete eriliikide, näiteks seksuaalse sättumuse, poliitiliste arvamuste ja usuliste veendumuste töötlemist, hõlmates seega laiaulatuslikku töötlemisvaldkonda. Lisaks puuduksid sellisel sättel konkreetsed nõuded, mis viitaksid asjaoludele ja tingimustele, mille korral õiguskaitseasutustel oleks õigus kasutada näotuvastustehnoloogiat. Kuna viidatakse muudele andmeliikidele ja spetsiifiliste kaitsemeetmete selgele vajadusele ilma täiendavate täpsustusteta, ei saa siseriiklikku sätet, millega võetakse

⁵² Kaalutavate seadusandlike meetmete liik peab olema kooskõlas ELi õigusega või siseriikliku õigusega. Sõltuvalt piirangu sekkumise ulatusest võidakse riigi tasandil nõuda konkreetset seadusandlikku meedet, võttes arvesse õigusnormi taset.

siseriiklikku õigusesse üle õiguskaitseDirektiivi artikkel 10 – sarnase üldise ja abstraktse sõnastusega – kasutada näotuvastust hõlmava biomeetriliste andmete töötlemise õigusliku alusena, sest see ei oleks täpne ega ettenähtav. Kooskõlas õiguskaitseDirektiivi artikli 28 lõikega 2 või artikli 46 lõike 1 punktiga c tuleks enne, kui seadusandja loob uue õigusliku aluse mis tahes vormis biomeetriliste andmete töötlemiseks näotuvastuse abil, konsulteerida riikliku andmekaitse järelevalveasutusega.

3.2.1.2 Rangelt vajalik

73. Töötlemist võib pidada „rangelt vajalikuks“ üksnes juhul, kui sekkumine isikuandmete kaitsesse ja selle piirangud piirduvad sellega, mis on absoluutselt vajalik⁵³. Mõiste „rangelt“ lisamine tähendab, et seadusandja soovis, et andmete eriliikide töötlemine toimuks üksnes tingimustel, mis on isegi rangemad kui vajalikkuse tingimused (vt eespool punkt 3.1.3.4). Seda nõuet tuleks tõlgendada hädavajalikkuna. See piirab õiguskaitseasutusele vajalikkuse kontrollimisel antud kaalutlusruumi absoluutse miinimumini. Euroopa Liidu Kohtu väljakujunenud kohtupraktika kohaselt on range vajalikkuse nõue tihedalt seotud ka nõudega objektiivsete kriteeriumide järele, mis võimaldaksid määrata kindlaks asjaolud ja tingimused, mille alusel saab töötlemist läbi viia, välistades seega üldise või süstemaatilise töötlemise⁵⁴.

3.2.1.3 Ilmselgelt avalikustatud

74. Kui hinnatakse, kas töötlemine on seotud andmesubjekti poolt ilmselgelt avalikustatud andmetega, tuleb meenutada, et fotot kui sellist ei käsitata süstemaatiliselt biomeetriliste andmetena⁵⁵. Seega ei tähenda asjaolu, et andmesubjekt on foto ilmselgelt avalikustanud, et sellega seotud biomeetrilised andmed, mida saab pildist konkreetsete tehniliste vahenditega hankida, loetakse ilmselgelt avalikustatuks.
75. Mis puudutab isikuandmeid üldiselt, siis selleks, et biomeetrilised andmed oleksid andmesubjekti poolt ilmselgelt avalikustatud, peab andmesubjekt olema tahtlikult teinud biomeetrilise malli (mitte lihtsalt näokujutise) avatud allika kaudu vabalt kättesaadavaks ja avalikuks. Kui kolmas isik avaldab biomeetrilised andmed, ei saa järeldada, et andmesubjekt on andmed ilmselgelt avalikustanud.
76. Samuti ei piisa andmesubjekti käitumise tõlgendamisest, et järeldada, et biomeetrilised andmed on ilmselgelt avalikustatud. Näiteks sotsiaalvõrgustike või veebiplatvormidega seoses leiab EDPB, et asjaolu, et andmesubjekt ei ole aktiveerinud ega seadistanud konkreetseid privaatsussätteid, ei ole piisav, et leida, et see andmesubjekt on ilmselgelt avalikustanud oma isikuandmed ning et neid andmeid (nt fotosid) võib töödelda biomeetrilisteks mallideks ja kasutada identifitseerimise eesmärgil ilma andmesubjekti nõusolekuta. Üldisemalt ei tohiks teenuse vaikesätteid, nt mallide avalikustamist, või valikuvõimaluse puudumist, nt mallid avalikustatakse, ilma et kasutaja saaks seda sätet muuta, mingil juhul tõlgendada kui andmete ilmselget avalikustamist.

⁵³ Väljakujunenud kohtupraktika eraelu puutumatuse põhiõiguse valdkonnas, vt Euroopa Liidu Kohtu otsus kohtuasjas C-73/07, punkt 56 (Satakunnan Markkinapörssi and Satamedia); kohtuasjades C-92/09 ja C-93/09, punkt 77 (Schecke and Eifert); kohtuasjas C-594/12, punkt 52 (Digital Rights); kohtuasjas C-362/14, punkt 92 (Schrems).

⁵⁴ Euroopa Liidu Kohtu otsus kohtuasjas C-623/17, punkt 78.

⁵⁵ Vt isikuandmete kaitse üldmääruse põhjendus 51: „[...] [f]otode töötlemist ei peaks süstemaatiliselt käsitlema isikuandmete eriliikide töötlemisena, kuna need on hõlmatud üksnes biomeetriliste andmete määratlusega, kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida.“

3.2.2 Automatiseeritud töötusel põhinevate üksikotsuste tegemine, sealhulgas profiilianalüüs

77. ÕiguskaitseDirektiivi artikli 11 lõikes 1 on sätestatud liikmesriikide kohustus üldiselt keelata otsused, mis põhinevad üksnes automatiseeritud töötusel, sealhulgas profiilianalüüsil, millel on andmesubjektile kahjulikud õiguslikud tagajärjed või märkimisväärne mõju. Erandina sellest üldisest keelust võib selline töötus olla võimalik üksnes juhul, kui seda lubab liidu või liikmesriigi õigus, mida kohaldatakse vastutavale töötlejale ja mis näeb ette andmesubjekti õiguste ja vabaduste sobivad kaitsemeetmed, vähemalt õiguse otseseks isiklikuks kontaktiks vastutava töötlejaga. Seda võib kasutada üksnes piiratud. Seda lävendit kohaldatakse tavaliste isikuandmete (st mitte isikuandmete eriliikide) suhtes. ÕiguskaitseDirektiivi artikli 11 lõike 2 kohasele erandile kehtivad veel kõrgem lävend ja piiravam kasutus. Selles rõhutatakse veel kord, et esimese lõigu alusel tehtavad otsused ei tohi põhineda andmete eriliikidel, st eelkõige biomeetrilistel andmetel, mille eesmärk on üheselt tuvastada füüsiline isik. Erandi võib ette näha ainult juhul, kui rakendatakse sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning konkreetse füüsilise isiku õigustatud huvide kaitseks. Seda erandit tuleb tõlgendada lisaks õiguskaitseDirektiivi artikli 10 eelduste kontekstis.
78. Sõltuvalt näotuvastussüsteemist ei pruugi isegi näotuvastustehnoloogia tulemusi hindav inimsekkumine iseenesest pakkuda piisavat tagatist üksikisikute õiguste ja eelkõige õiguse isikuandmete kaitseks, arvestades võimalikku kallutatust ja töötlemisest endast potentsiaalselt tulenevat eksimust. Lisaks võib inimsekkumist pidada kaitsemeetmeks üksnes juhul, kui sekkuv isik võib inimsekkumise käigus näotuvastustehnoloogia tulemused kriitiliselt vaidlustada. On väga oluline, et isik mõistaks näotuvastussüsteemi ja selle piiranguid ning tõlgendaks selle tulemusi õigesti. Samuti on vaja luua tööpaik ja -korraldus, mis tasakaalustaksid automatiseerimise eelistamist ning väldiksid tulemuste kriitikata aktsepteerimist näiteks ajasurve, koormavate menetluste, võimaliku kahjuliku karjäärimõju jms tõttu.
79. ÕiguskaitseDirektiivi artikli 11 lõike 3 alusel on profiilianalüüs, mille tulemusel füüsilisi isikuid diskrimineeritakse isikuandmete eriliikide, nt biomeetriliste andmete alusel, kooskõlas liidu õigusega keelatud. ÕiguskaitseDirektiivi artikli 3 lõike 4 kohaselt tähendab profiilianalüüs igasugust isikuandmete automatiseeritud töötlemist, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud kõnealuse füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega. Kui kaalutakse sobivaid meetmeid andmesubjekti õiguste ja vabaduste ning puudutatud füüsilise isiku õigustatud huvide kaitseks, tuleb arvestada, et näotuvastustehnoloogia kasutamine võib viia profiilianalüüsini, sõltuvalt sellest, mis viisil ja eesmärgil seda tehnoloogiat kohaldatakse. Igal juhul on vastavalt liidu õigusele ja õiguskaitseDirektiivi artikli 11 lõikele 3 keelatud profiilianalüüs, mille tulemusel füüsilisi isikuid diskrimineeritakse isikuandmete eriliikide alusel.

3.2.3 Andmesubjektide kategooriad

80. ÕiguskaitseDirektiivi artikkel 6 käsitleb vajadust teha vahet erinevate andmesubjektide kategooriate vahel. Sellist eristamist tuleb kohaldada asjakohasel juhul ja võimalikult suures ulatuses. See peab kajastuma andmete töötlemise viisis. ÕiguskaitseDirektiivi artiklis 6 esitatud näidete põhjal võib järeldada, et reeglina peab isikuandmete töötlemine vastama vajalikkuse ja proportsionaalsuse kriteeriumidele ka seoses andmesubjektide kategooriaga⁵⁶. Lisaks võib järeldada, et kui andmesubjektide kohta puuduvad tõendid, mis viitaksid sellele, et nende tegevusel võib olla kasvõi kaudne seos õiguskaitseDirektiivi kohase õiguspärase eesmärgiga, ei ole sekkumine tõenäoliselt

⁵⁶ Vt ka Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punktid 56–59.

põhjendatud⁵⁷. Kui õiguskaitseDirektiivi artikli 6 kohane eristamine ei ole kohaldatav ega võimalik, tuleb sekkumise vajalikkuse ja proportsionaalsuse hindamisel rangelt arvestada direktiivi artiklis 6 sätestatud reegli erandit. Erinevate andmesubjektide kategooriate eristamine on näotuvastust hõlmaval isikuandmete töötlemisel oluline nõue, võttes arvesse ka võimalikke valepositiivseid või valenegatiivseid tulemusi, millel võib olla märkimisväärne mõju nii andmesubjektidele kui ka uurimise käigule.

81. Nagu öeldud, tuleb liidu õiguse rakendamisel järgida Euroopa Liidu põhiõiguste harta sätteid (vt harta artikkel 52). Seetõttu tuleb õiguskaitseDirektiivis sätestatud raamistikku ja kriteeriume tõlgendada harta kontekstis. ELi ja selle liikmesriikide õigusaktid ei tohi olla sellest meetmest nõrgema mõjuga ning peavad tagama harta täieliku õigusmõju.

3.2.4 Andmesubjekti õigused

82. EDPB on juba andnud juhiseid isikuandmete kaitse üldmäärusest tulenevate andmesubjektide õiguste eri aspektide kohta⁵⁸. ÕiguskaitseDirektiiv näeb ette sarnased andmesubjektide õigused ning EDPB poolt heakskiidetud üldsuunised on esitatud ka artikli 29 töörühma arvamuses⁵⁹. ÕiguskaitseDirektiiv võimaldab kehtestada nende õiguste piiranguid teatavatel tingimustel. Selliste piirangute parameetreid on täpsemalt kirjeldatud punktis 3.2.4.6. „Andmesubjektide õiguste õiguspärased piirangud“.
83. Kuigi kõik andmesubjektide õigused, mis on loetletud õiguskaitseDirektiivi III peatükis, kehtivad loomulikult ka näotuvastustehnoloogiat kasutaval isikuandmete töötlemisel, keskendutakse järgnevas peatükis teatavatele õigustele ja aspektidele, mille kohta suuniste saamine võib pakkuda erilist huvi. Pealegi lähtuvad see peatükk ja siin esitatud analüüs eeldusest, et näotuvastustehnoloogiat kasutav töötlemine järgib eelmises peatükis kirjeldatud õiguslikke nõudeid.
84. Võttes arvesse näotuvastustehnoloogiat kasutava isikuandmete töötlemise olemust (isikuandmete eriliikide töötlemine sageli ilma andmesubjektiga mingil viisil suhtlemata), peab vastutav töötleja enne sellise töötlemise alustamist hoolikalt kaaluma, kuidas (või kas) ta saab täita õiguskaitseDirektiivi nõudeid. Eelkõige peab ta hoolikalt analüüsima järgmist:
- kes on andmesubjektid (sageli hõlmab suuremat arvu isikuid kui töötlemise peamist sihtrühma);
 - kuidas andmesubjekte näotuvastustehnoloogiat kasutavast töötlemisest teavitatakse (vt punkt 3.2.4.1);
 - kuidas andmesubjektid saavad kasutada oma õigusi (siinkohal võib olla eriti keeruline tagada nii teavitamis- kui ka tutvumisõigust kui ka õigust andmete parandamisele või töötlemise piiramisele juhul, kui näotuvastustehnoloogiat kasutatakse muudeks rakendusteks kui üks-ühele kontrolliks otseses suhtluses andmesubjektiga).

3.2.4.1 Õiguste ja teabe andmesubjektidele teatavaks tegemine kokkuvõtlikul, arusaadaval ja kergesti kättesaadaval kujul

85. Näotuvastustehnoloogia kasutamisel on keeruline tagada, et andmesubjektid oleksid oma biomeetriliste andmete töötlemisest teadlikud. Eriti keeruline on see siis, kui õiguskaitseasutus analüüsib näotuvastustehnoloogia abil videomaterjali, mis pärineb või on saadud kolmandalt isikult, sest õiguskaitseasutusel on vähe võimalusi ja enamikul juhtudel puudub üldse võimalus andmesubjekti

⁵⁷ Vt ka Euroopa Liidu Kohtu otsus kohtuasjas C-594/12, punkt 58.

⁵⁸ Vt näiteks 1/2022 EDPB suunised andmesubjektide õiguste (andmetega tutvumise õiguse) kohta ning 3/2019 EDPB suunised isikuandmete töötlemise kohta videoseadmetes.

⁵⁹ WP258, arvamus õiguskaitseDirektiivi (EL 2016/680) teatavate põhiküsimuste kohta.

andmete kogumise ajal teavitada (nt kohapealse sildiga). Igasugune videomaterjal, mis ei ole uurimise (või töötlemise eesmärgi) seisukohast asjakohane, tuleks enne biomeetriliste andmete töötlemise alustamist alati kõrvaldada või anonüümiseerida (nt hägustades andmed ilma tagasiulatuva taastamise võimaluseta), et vältida riski, et ei täideta õiguskaitseDirektiivi artikli 4 lõike 1 punktis e sätestatud võimalikult väheste andmete kogumise põhimõtet ja õiguskaitseDirektiivi artikli 13 lõikes 2 sätestatud teavitamiskohustusi. Vastutava töötleja ülesanne on hinnata, milline teave oleks andmesubjekti jaoks oluline tema õiguste kasutamisel, ja tagada, et vajalik teave esitataks. Andmesubjekti õiguste tõhus kasutamine sõltub sellest, kas vastutav töötleja täidab oma teavitamiskohustusi.

86. ÕiguskaitseDirektiivi artikli 13 lõikes 1 on sätestatud andmesubjektile üldiselt esitatav miinimumteave. Selle teabe võib esitada vastutava töötleja veebilehel, trükisena (nt nõudmisel kättesaadav teabeleht) või andmesubjektile muul viisil kergesti juurdepääsetavate allikate kaudu. Vastutav töötleja peab igal juhul tagama, et tõepoolest esitataks vähemalt järgmised andmed:
- vastutava töötleja, sh andmekaitseSpetsialisti nimi ja kontaktandmed;
 - töötlemise eesmärk ja asjaolu, et töötlemine toimub näotuvastustehnoloogia abil;
 - õigus esitada järelevalveasutusele kaebus ja sellise asutuse kontaktandmed;
 - õigus taotleda isikuandmetega tutvumist, nende parandamist või kustutamist ning isikuandmete töötlemise piiramist.
87. Lisaks tuleb siseriiklikus õiguses määratletud erijuhtudel, mis peaksid olema kooskõlas õiguskaitseDirektiivi artikli 13 lõikega 2⁶⁰, näiteks näotuvastustehnoloogiat kasutava töötlemise korral, esitada andmesubjektile otse järgmine teave:
- töötlemise õiguslik alus;
 - teave, kust isikuandmed koguti ilma andmesubjekti teadmata;
 - ajavahemik, mille jooksul isikuandmeid säilitatakse, või, kui see ei ole võimalik, siis sellise ajavahemiku kindlaksmääramise kriteeriumid;
 - vajadusel isikuandmete vastuvõtjate kategooriad (sh kolmandad riigid või rahvusvahelised organisatsioonid).
88. Kui õiguskaitseDirektiivi artikli 13 lõige 1 käsitleb üldsusele kättesaadavaks tehtavat üldist teavet, siis selle artikli 13 lõige 2 käsitleb täiendavat teavet, mis tuleb konkreetsele andmesubjektile teatavatel juhtudel esitada, nt kui andmeid kogutakse otse andmesubjektilt või kaudselt ilma andmesubjekti teadmata⁶¹. ÕiguskaitseDirektiivi artikli 13 lõikes 2 ei ole selgelt määratletud, mida mõeldakse „konkreetsete juhtude“ all. See viitab aga olukordadele, kus andmesubjekte tuleb teavitada neid konkreetselt puudutavast töötlemisest ja neile tuleb anda asjakohast teavet, et nad saaksid oma õigusi tõhusalt kasutada. EDPB on seisukohal, et „konkreetsede juhtumite“ olemasolu hindamisel tuleb arvesse võtta mitmeid tegureid, sealhulgas kas isikuandmeid kogutakse andmesubjekti teadmata, sest see oleks ainus viis, kuidas andmesubjektid saaksid oma õigusi tõhusalt kasutada. Muud „konkreetsete juhtude“ näited võivad olla juhtumid, kus isikuandmeid töödeldakse edasi rahvusvahelise kriminaalkoostöö menetluse või varjatud operatsioonide toimingute raames, mis on sätestatud liikmesriigi õiguses. Lisaks tuleneb õiguskaitseDirektiivi põhjendusest 38, et kui otsuseid tehakse

⁶⁰ Nt Saksamaa föderalse andmekaitseSeaduse artikli 56 lõige 1, milles on muu hulgas sätestatud, mis teavet tuleb andmesubjektidele anda varjatud toimingute korral.

⁶¹ WP258, arvamus õiguskaitseDirektiivi (EL 2016/680) teatavate põhiküsimuste kohta, lk 17–18.

üksnes näotuvastustehnoloogiat kasutava töötlemise alusel, tuleb andmesubjekte teavitada automatiseeritud töötusel põhineva otsuste tegemise tingimustest. See viitab ühtlasi sellele, et tegemist on konkreetse juhtumiga, mille korral tuleks andmesubjektile esitada täiendavat teavet kooskõlas õiguskaitseDirektiivi artikli 13 lõikega 2⁶².

89. Lisaks tuleb märkida, et õiguskaitseDirektiivi artikli 13 lõike 3 kohaselt võivad liikmesriigid võtta seadusandlikke meetmeid, millega piiratakse teavitamiskohustust konkreetsetel juhtudel teatavatel eesmärkidel. See kehtib sellises ulatuses ja seni, kui selline meede on demokraatlikus ühiskonnas vajalik ja proportsionaalne, võttes nõuetekohaselt arvesse andmesubjekti põhiõigusi ja õigustatud huve.

3.2.4.2 Õigus andmetega tutvuda

90. Üldiselt on andmesubjektil õigus saada vastutavalt töötlejalt kinnitus, kas teda käsitlevaid isikuandmeid töödeldakse või mitte, ning nende töötlemise korral on andmesubjektil õigus tutvuda isikuandmete ja teabega, mis on loetletud õiguskaitseDirektiivi artiklis 14. Kui kasutatakse näotuvastust ja kui biomeetrilised andmed on salvestatud ja seotud identiteediga ka tähtnumbriliste andmete abil, peaks see võimaldama pädeval asutusel anda kinnitus tutvumistaotlusele nende tähtnumbriliste andmete otsingu põhjal ilma teiste isikute biomeetriliste andmete edasist töötlemist alustamata (s.t otsides näotuvastustehnoloogia abil andmebaasis). Tuleb järgida võimalikult väheste andmete töötlemise põhimõtet ning ei tohi säilitada rohkem andmeid, kui on vaja seoses töötlemise eesmärgiga.

3.2.4.3 Õigus isikuandmete parandamisele

91. Kuna näotuvastustehnoloogia ei taga absoluutset täpsust, on eriti oluline, et vastutavad töötlejad oleksid isikuandmete parandamise taotluste suhtes valvsad. Võib ka juhtuda, et andmesubjekt on näotuvastustehnoloogia alusel liigitatud valesse kategooriasse, nt kui ta on videomaterjalist lähtuva esialgse oletuse põhjal ebaõigesti liigitatud kahtluseluste kategooriasse. Andmesubjektidele avalduvad ohud on eriti suured, kui selliseid ebatäpseid andmeid säilitatakse politsei andmebaasis ja/või jagatakse teiste üksustega. Vastutav töötleja peab salvestatud andmeid ja näotuvastussüsteeme vastavalt parandama, vt õiguskaitseDirektiivi põhjenduspunkti 47.

3.2.4.4 Õigus andmete kustutamisele

92. Näotuvastustehnoloogia tähendab enamikul juhtudel – juhul kui seda ei kasutata üks-ühele kontrolliks/autentimiseks – suure hulga andmesubjektide biomeetriliste andmete töötlemist. Seetõttu on oluline, et vastutav töötleja kaaluks eelnevalt selle töötlemise eesmärgi ja vajalikkuse piire, et õiguskaitseDirektiivi artikli 16 kohast kustutamistaotlust saaks käsitleda põhjendamatult viivitusega (sest vastutav töötleja peab muu hulgas kustutama isikuandmed, mida töödeldakse ulatuslikumalt, kui kehtivad õigusaktid õiguskaitseDirektiivi artiklite 4, 8 ja 10 alusel lubavad).

3.2.4.5 Õigus töötlemise piiramisele

93. Kui andmesubjekt vaidlustab andmete õigsust ja andmete õigsust ei ole võimalik kindlaks teha (või kui isikuandmeid tuleb säilitada tõendamise eesmärgil), on vastutaval töötlejal kohustus piirata andmesubjekti isikuandmete töötlemist kooskõlas õiguskaitseDirektiivi artikliga 16. See on eriti oluline, kui tegemist on näotuvastustehnoloogiaga (mis põhineb algoritmi(de)l ja ei anna seega kunagi lõplikku tulemust) olukordades, kus kogutakse suuri hulki andmeid ning tuvastamise õigsus ja kvaliteet võivad varieeruda. Halva kvaliteediga (nt kuriteopaigast pärit) videomaterjali kasutamisel suureneb valepositiivsete tulemuste risk. Ka jälgimisnimekirjas olevate näokujutiste ebaregulaarne ajakohastamine suurendab valepositiivsete või valenegatiivsete tulemuste riski. Konkreetsetel

⁶² Pange tähele erinevust õiguskaitseDirektiivi artikli 13 lõikes 1 märgitud „andmesubjektile kättesaadavaks tehtud“ ja selle lõikes 2 märgitud „annab[...]talle“ vahel. ÕiguskaitseDirektiivi artikli 13 lõike 2 kohaselt peab vastutav töötleja tagama, et teave jõuaks andmesubjektini, kui veebilehel avaldatud teabest ei piisa.

juhtudel, kui andmeid ei saa kustutada, sest on põhjendatud alus arvata, et kustutamine võib kahjustada andmesubjekti õigustatud huve, tuleks selle asemel andmete töötlemist piirata ja töödelda neid üksnes sel eesmärgil, mis takistas kustutamist (vt õiguskaitse direktiivi põhjendus 47).

3.2.4.6 Andmesubjekti õiguste õiguspärased piirangud

94. Mis puudutab vastutava töötleja teavitamiskohustust ja andmesubjektide õigusega tutvuda andmetega, siis on piirangud lubatud üksnes juhul, kui need on sätestatud seaduses, mis omakorda peab olema demokraatlikus ühiskonnas puudutatud füüsilise isiku põhiõigusi ja õigustatud huve nõuetekohaselt arvesse võttes vajalik ja proportsionaalne meede (vt õiguskaitse direktiivi artikli 13 lõiked 3 ja 4, artikkel 15 ning artikli 16 lõige 4). Kui näotuvastustehnoloogiat kasutatakse õiguskaitse eesmärkidel, võib eeldada, et seda kasutatakse olukorras, kus andmesubjekti teavitamine või andmetega tutvumise võimaldamine oleks taotletava eesmärgi saavutamiseks kahjulik. See kehtib näiteks politsei uurimine kuriteo kohta või riigi julgeoleku või avaliku julgeoleku kaitse kohta.
95. Andmetega tutvumise õigus ei tähenda automaatselt juurdepääsu kogu teabele, näiteks kriminaalasjas, mille raames isikuandmeid koguti. Sobiv näide, millal võib lubada selle õiguse piiramist, oleks kriminaaluurimine.

3.2.4.7 Õiguste kasutamine järelevalveasutuse kaudu

96. Juhtudel, kus õiguskaitse direktiivi III peatüki kohaste õiguste kasutamine on õiguspäraselt piiratud, võib andmesubjekt taotleda, et andmekaitseasutus kasutaks tema õigusi tema eest, kontrollides vastutava töötleja poolse töötlemise seaduslikkust. Vastutav töötleja peab andmesubjekti teavitama võimalusest kasutada oma õigusi sellisel viisil (vt õiguskaitse direktiivi artikkel 17 ja artikli 46 lõike 1 punkt g). Seoses näotuvastustehnoloogiaga tähendab see, et vastutav töötleja peab tagama asjakohased meetmed sellise taotluse käsitlemiseks, näiteks võimaldama otsingut salvestatud materjalis, kui andmesubjekt annab oma isikuandmete leidmiseks piisavalt teavet.

3.2.5 Muud õiguslikud nõuded ja kaitsemeetmed

3.2.5.1 Artikkel 27. Andmekaitsealane mõjuhindang

97. Enne näotuvastustehnoloogia kasutamist on kohustuslik teha andmekaitsealane mõjuhindang, sest isikuandmete töötlemise viis, eelkõige uute tehnoloogiate kasutamine, ning töötlemise laad, ulatus, kontekst ja eesmärgid võivad tõenäoliselt oluliselt ohustada füüsiliste isikute õigusi ja vabadusi. Kuivõrd näotuvastustehnoloogia kasutamine hõlmab andmete eriliikide süstemaatilist automaatset töötlemist, võib eeldada, et vastutav töötleja on sellisel juhul reeglina kohustatud tegema andmekaitsealase mõjuhindangu. Andmekaitsealane mõjuhindang peaks sisaldama vähemalt kavandatud töötlemistoimingute üldist kirjeldust, töötlemistoimingute vajalikkuse ja proportsionaalsuse hinnangut seoses eesmärkidega, andmesubjektide õigustele ja vabadustele avalduvate ohtude hinnangut, nende ohtude leevendamiseks kavandatud meetmeid, kaitsemeetmeid, turvameetmeid ja -mehhanisme, et tagada isikuandmete kaitse ja tõendada nõuetele vastavust. EDPB soovib usalduse ja läbipaistvuse suurendamise meetmena avalikustada selliste hinnangute tulemused või vähemalt andmekaitse mõjuhindangu põhilised järeldused⁶³.

3.2.5.2 Artikkel 28. Eelnev konsulteerimine järelevalveasutusega

98. Õiguskaitse direktiivi artikli 28 kohaselt peab vastutav töötleja või volitatud töötleja enne töötlemist konsulteerima järelevalveasutusega, kui: a) andmekaitsealasest mõjuhindangust nähtub, et töötlemise tulemusena tekiks vastutava töötleja poolt ohu leevendamiseks võetavate meetmete puudumise korral suur oht, või b) töötlemise laadiga, eelkõige kui kasutatakse uusi tehnoloogiaid,

⁶³ Lisateave on dokumendis WP248 rev.01 „Suunised, mis käsitlevad andmekaitsealasest mõjuhindangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena tõenäoliselt „tekib suur oht““.

mehhanisme või menetlusi, kaasneb suur oht andmesubjekti õigustele ja vabadustele. Nagu on selgitatud käesolevate suuniste punktis 2.3, leiab EDPB, et enamiku näotuvastustehnoloogia rakendamise ja kasutamise juhtumitega kaasneb olemuslikult suur oht andmesubjektide õigustele ja vabadustele. Seepärast peaks seda tehnoloogiat rakendav asutus lisaks andmekaitsealase mõjuhinna koostamisele konsulteerima enne süsteemi kasutuselevõttu pädeva järelevalveasutusega.

3.2.5.3 Artikkel 29. Isikuandmete töötlemise turvalisus

99. Biomeetriliste andmete ainulaadsuse tõttu ei ole andmesubjektil võimalik neid muuta, kui need on ohus, näiteks andmetega seotud rikkumise tõttu. Seetõttu peaks pädev asutus, kes näotuvastustehnoloogiat rakendab ja/või kasutab, pöörama kooskõlas õiguskaitse direktiivi artikliga 29 erilist tähelepanu töötlemise turvalisusele. Eelkõige peaks õiguskaitseasutus tagama, et süsteem vastaks asjakohastele standarditele, ja rakendama biomeetriliste mallide kaitse meetmeid⁶⁴. See kohustus on veelgi olulisem, kui õiguskaitseasutus kasutab kolmandast isikust teenuseosutajat (volitatud töötajat).

3.2.5.4 Artikkel 20. Lõimitud ja vaikimisi andmekaitse

100. Õiguskaitse direktiivi artikli 20 kohase lõimitud ja vaikimisi andmekaitse eesmärk on tagada, et andmekaitse põhimõtted ja kaitsemeetmed, näiteks võimalikult väheste andmete kogumine ja säilitamispiirang, integreeritaks tehnoloogiasse asjakohaste tehniliste ja korralduslike meetmete abil, nt pseudonümiseerimine, juba enne isikuandmete töötlemise algust, ja et neid rakendataks kogu selle olulusringi jooksul. Arvestades füüsiliste isikute õigustele ja vabadustele avalduvat suurt riski, ei tohiks selliste meetmete valik sõltuda üksnes majanduslikest kaalutlustest⁶⁵, vaid selle asemel tuleks püüda rakendada uusimat andmekaitsetehnoloogiat. Samamoodi peab õiguskaitseasutus, kui ta kavatses kohaldada ja kasutada väliste teenuseosutajate pakutavat näotuvastustehnoloogiat, tagama näiteks hankemenetluse kaudu, et kasutusele võetaks üksnes lõimitud ja vaikimisi andmekaitse põhimõtetele tuginev näotuvastustehnoloogia⁶⁶. See tähendab ühtlasi, et näotuvastustehnoloogia toimimise läbipaistvust ei piira ärisaladuste või intellektuaalomandi õiguste kaitse.

3.2.5.5 Artikkel 25. Logimine

101. Õiguskaitse direktiivis on sätestatud erinevad meetodid, mille abil vastutav töötaja või volitatud töötaja tõendab töötlemise seaduslikkust ning tagab andmete tervikluse ja turvalisuse. Selles osas on süsteemiligid väga kasulik vahend ja oluline kaitsemeede töötlemise seaduslikkuse kontrollimiseks nii asutusesiseselt (st siseseire) kui ka väliste järelevalveasutuste, näiteks andmekaitseasutuste poolt. Vastavalt õiguskaitse direktiivi artiklile 25 tuleks automatiseeritud töötlemissüsteemides säilitada vähemalt järgmiste töötlemistoimingute logid: kogumine, muutmine, lugemine, avalikustamine (sh edastamine), ühendamine ja kustutamine. Lisaks peaks andmetega tutvumise ja avalikustamise logide abil olema võimalik kindlaks teha selliste toimingute põhjendus, kuupäev ja kellaaeg ning võimalusel tuvastada isik, kes isikuandmetega tutvus või need avalikustas, ning selliste isikuandmete vastuvõtjad. Peale selle soovitatakse näotuvastussüsteemide kontekstis logida järgmised täiendavad töötlemistoimingud (osaliselt ületavad õiguskaitse direktiivi artikli 25 loetelu):

⁶⁴ Vt näiteks: ISO/IEC 24745 „Infoturvet, küberturvalisus ja privaatsuse kaitse – biomeetrilise teabe kaitse“.

⁶⁵ Vt õiguskaitse direktiivi põhjendus 53.

⁶⁶ Lisateave on EDPB suunistes lõimitud ja vaikimisi andmekaitse kohta, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

- Võrdlusandmebaasi muudatused (lisamine, kustutamine või ajakohastamine). Logi peaks säilitama asjakohase (lisatud, kustutatud või ajakohastatud) kujutise koopiat, kui töötlemistoimingute seaduslikkust või tulemust ei ole võimalik muul viisil kontrollida.
- Tuvastamis- või kontrollikatsed, sealhulgas tulemused ja usaldusväärsuse skoor. Võimalikult väheste andmete kogumise põhimõtet tuleks kohaldada rangelt, nii et viitekujutise säilitamise asemel säilitataks logides ainult võrdlusandmebaasist pärit kujutise identifikaator. Sisestatud biomeetriliste andmete logimist tuleks vältida, v.a kui see on vajalik (nt ainult kokkulangevuse hindamise juhtumitel korral).
- Kasutaja ID, kes tegi identifitseerimis- või kontrollimiskatse.
- Süsteemilogides säilitatavatele isikuandmetele kehtivad ranged eesmärgipiirangud (nt auditid) ja neid ei tohiks kasutada muudel eesmärkidel (nt selleks, et endiselt teostada tuvastamist/kontrollimist, sealhulgas võrdlusandmebaasidest kustutatud kujutisega). Logide terviklikkuse tagamiseks tuleks kohaldada turvameetmeid; väga soovitatav on kasutada ka automaatseid seiresüsteeme logide kuritarvitamise tuvastamiseks. Võrdlusandmebaasi logide turvameetmed peaksid olema näokujutiste säilitamise korral samaväärsed võrdlusandmebaasiga. Samuti tuleks rakendada automatiseeritud protsesse, et tagada andmete säilitamise perioodi järgimine logide puhul.

3.2.5.6 Artikli 4 lõige 4. Vastutus

102. Vastutav töötleja peab suutma tõendada, et töötlemine vastab õiguskaitse direktiivi artikli 4 lõigetes 1–3 sätestatud põhimõtetele (vt artikli 4 lõige 4). Seejuures on äärmiselt oluline süsteemi süstemaatiline ja ajakohane dokumenteerimine (sh ajakohastused, uuendused ja algoritmi õpetamine), tehnilised ja korralduslikud meetmed (sh süsteemi toimivuse jälgimine ja võimalik inimsekkumine) ning isikuandmete töötlemine. Töötlemise õiguspärasuse tõendamiseks on logimine eriti oluline element vastavalt õiguskaitse direktiivi artiklile 25 (vt punkt 3.2.5.5). Vastutuse põhimõte ei ole seotud üksnes süsteemi ja andmetöötlusega, vaid ka menetluslike kaitsemeetmete, näiteks vajalikkuse ja proportsionaalsuse hindamise, andmekaitsealaste mõjuhinnaangute ja ka sisemiste konsultatsioonide (nt projekti heakskiit juhtkonna poolt või usaldusväärsuse skooore käsitlevad sisemised otsused) ja väliste konsultatsioonide (nt andmekaitseasutustega) dokumenteerimisega. II lisa sisaldab sellega seoses mitmeid elemente.

3.2.5.7 Artikkel 47. Tõhus järelevalve

103. Pädevate andmekaitseasutuste poolt teostatav tõhus järelevalve on üks olulisemaid kaitsemeetmeid näotuvastustehnoloogia kasutamisest mõjutatud isikute põhiõiguste ja -vabaduste kaitseks. Samas on andmekaitseasutustele vajaliku personali, tehniliste ja rahaliste ressursside, ruumide ja taristu tagamine nende ülesannete tulemusliku täitmise ja volituste kasutamise eeltingimus⁶⁷. Veel olulisem kui olemasoleva personali arv on ekspertide oskused, mis peaksid hõlmama väga laia teemaderingi – alates kriminaaluurimistest ja politseikoostööst kuni suurandmete analüüsi ja tehisintellektini. Seetõttu peaksid liikmesriigid tagama, et järelevalveasutuste ressursid oleks asjakohased ja piisavad, et nad saaksid täita oma volitusi andmesubjektide õiguste kaitsmisel ning jälgiksid tähelepanelikult kõiki arenguid selles valdkonnas.⁶⁸

⁶⁷ Vt komisjoni teatis „Esimene aruanne õiguskaitse valdkonnas isikuandmete kaitset käsitleva direktiivi (EL) 2016/680 (õiguskaitse direktiiv) kohaldamise ja toimimise kohta“, COM(2022) 364 final, punkt 3.4.1.

⁶⁸ Vt EDPB panus õiguskaitse direktiivi artikli 62 kohasesse hindamisse Euroopa Komisjoni poolt, punkt 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf

4 JÄRELDUS

104. Näotuvastustehnoloogiate kasutamine on lahutamatult seotud suure hulga isikuandmete, sealhulgas andmete eriliikide töötlemisega. Nägu ja üldisemalt biomeetrilised andmed on püsivalt ja pöördumatult seotud isiku identiteediga. Seetõttu mõjutab näotuvastustehnoloogia kasutamine otseselt või kaudselt mitmeid Eli põhiõiguste hartas sätestatud põhiõigusi ja -vabadusi, mis võivad ulatuda kaugemale kui eraelu puutumatuse ja andmekaitse, mõjutades inimväärikust, liikumisvabadust, kogunemisvabadust jne. See on eriti oluline õiguskaitse ja kriminaalõiguse valdkonnas.
105. EDPB mõistab, et õiguskaitseasutustel on vaja kasutada parimaid võimalikke vahendeid, et kiiresti kindlaks teha terroriaktide ja muude raskete kuritegude toimepanijad. Selliseid vahendeid tuleks siiski kasutada rangelt kooskõlas kohaldatava õigusraamistikuga ja üksnes juhul, kui need vastavad harta artikli 52 lõikes 1 sätestatud vajalikkuse ja proportsionaalsuse nõuetele. Ehkki nüüdisaegsed tehnoloogiad võivad olla suureks abiks, ei ole need mingi kiire lahendus.
106. Teatud näotuvastustehnoloogia kasutamise juhtumid tekitavad üksikisikutele ja ühiskonnale liiga suuri riske. Neil põhjustel nõuavad EDPB ja Euroopa Andmekaitseinspektor nende üldist keelustamist⁶⁹.
107. Eelkõige kaasneb isikute biomeetrilise kaugtuvastamisega avalikes kohtades suur oht sekkuda üksikisikute eraellu ning sel ei ole kohta demokraatlikus ühiskonnas, sest see toob oma olemuselt kaasa isikute massilise jälgimise. Samuti leiab EDPB, et tehisintellektipõhised näotuvastussüsteemid, mis liigitavad isikuid nende biomeetriliste andmete alusel etnilise päritolu, soo, poliitilise või seksuaalse sättumuse järgi klastritesse, ei ole kooskõlas hartaga. Lisaks on EDPB veendunud, et näotuvastuse või sarnaste tehnoloogiate kasutamine füüsiliste isikute emotsioonide tuletamiseks on äärmiselt ebasoovitav ja peaks olema keelatud, potentsiaalselt mõne nõuetekohaselt põhjendatud erandiga. Lisaks leiab EDPB, et õiguskaitse kontekstis toimuv isikuandmete töötlemine, mis tugineb andmebaasile, milles sisalduvad isikuandmed on kogutud massiliselt ja andmesubjekte mitteeristavalt, nt internetis, eriti sotsiaalsõrgustikes kättesaadavate fotode ja näopiltide „koorimise“ teel, ei vasta sellisena liidu õiguses sätestatud vajalikkuse rangele nõudele.

5 LISAD

I lisa. Tugimuster

II lisa. Praktilised suunised näotuvastustehnoloogia projektide juhtimiseks õiguskaitseasutustes

III lisa. Praktilised näited

⁶⁹ Vt EDPB ja Euroopa Andmekaitseinspektori ühine ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid (tehisintellekti käsitlev õigusakt) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

I LISA. STSENAARIUMIDE KIRJELDAMISE VORM

(koos infokastidega stsenaariumide raames käsitletud aspektidega)

Töötlemise kirjeldus

- Töötlemise kirjeldus, kontekst (seos kuriteoga), eesmärk

Teabe allikas

- Andmesubjektide liigid: ☐ kõik kodanikud ☐ süüdimõistatud ☐ kahtlusalsused
☐ lapsed ☐ muud haavatavad andmesubjektid
- Kujutise allikas: ☐ avalikud kohad ☐ internet
☐ eraõiguslik üksus ☐ teised üksikisikud ☐ muu
- Seos kuriteoga: ☐ otsene ajaline seos ☐ otsene ajaline seos puudub
☐ otsene geograafiline seos ☐ otsene geograafiline seos puudub
☐ ei ole vajalik
- Teabe kogumise viis: ☐ kaugmeetod ☐ kabiinis või kontrollitud keskkonnas
- Kontekst – mõju teistele põhiõigustele:
☐ ei
jah, nimelt ☐ kogunemisvabadus
☐ sõnavabadus
☐ muud mitmed õigused:.....
- Võimalikud lisaallikad andmesubjektiga seotud teabe kogumiseks
☒ isikut tõendav dokument ☐ avalik telefoni kasutamine ☐ sõiduki
numbrimärk
☐ muu

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☐ üldotstarbelised andmebaasid ☐
kuriteovaldkonnaga seotud erandmebaasid
- Kirjeldus sellest, kuidas võrdlusandmebaasid täideti (ja õiguslik alus)
- Andmebaasi otstarbe muutus (nt põhieesmärk oli eraomandi turvalisus): ☐ JAH
☐ EI

Algoritm

- Töötlemise liik: ☐ üks-ühele kontrollimine (autentimine) ☐ üks-mitmele tuvastamine
- Andmete õigsusega seotud kaalutlused
- Tehnilised kaitsemeetmed

Tulemus

- Mõju ☐ otsene (nt andmesubjekti võidakse vahistada, küsitleda, kohelda diskrimineerivalt)
☐ mitteotsene (andmeid kasutatakse statistilistes mudelites, andmesubjektidele ei
teki tõsised õiguslike tagajärgi)
- Automatiseeritud töötlusel põhinev otsus: ☐ JAH ☐ EI

- Säilitamise kestvus

Õiguslik analüüs

- Vajalikkuse ja proportsionaalsuse analüüs – kuriteo eesmärk / raskusaste / isikute arv, keda töötlemine mõjutab
- Andmesubjektile eelnevalt edastatud teabe liik:
 - ☐ konkreetsele alasse sisenemisel
 - ☐ õiguskaitseasutuse veebilehel üldiselt
 - ☐ õiguskaitseasutuse veebilehel konkreetse

töötlemise kohta

☐ muu

- Kohaldatav õigusraamistik:

☐ siseriikliku õigusesse ülevõetud õiguskaitse direktiiv

☐ üldine siseriiklik õigus, mis käsitleb biomeetriliste andmete kasutamist

õiguskaitseasutuste poolt

☐ konkreetne siseriiklik õigusakt mis käsitleb selles pädevas asutuses kõnealust töötlemist (näotuvastus)

☐ konkreetne siseriiklik õigusakt mis käsitleb kõnealust töötlemist

(automatiseeritud töötlusel põhinev otsus)

Kokkuvõte

Üldised kaalutlused, kas kirjeldatud töötlemine on tõenäoliselt kooskõlas ELi õigusega (ja mõned vihjed õiguslikele eeltingimustele)

II LISA. PRAKTILISED SUUNISED NÄOTUVASTUSTEHNOLLOOGIA PROJEKTIDE JUHTIMISEKS ÕIGUSKAITSEASUTUSTES

Selles lisas esitatakse täiendavad suunised õiguskaitseasutustele, kes plaanivad alata näotuvastustehnoloogiat hõlmava projekti. Selles antakse lisateavet korralduslike ja tehniliste meetmete kohta, mida võiks projekti rakendamise ajal kaaluda, kuid see meetmete loetelu ei ole ammendav. Lisaks tuleks arvesse võtta EDPB [suuniseid 3/2019 isikuandmete töötlemise kohta videoseadmetes](#)⁷⁰ ning mis tahes ELi/EMP eeskirju ja EDPB suuniseid tehisintellekti kasutamise kohta.

Selles lisas esitatud suunised põhinevad eeldusel, et õiguskaitseasutused hangivad näotuvastustehnoloogiat (valmistootena). Kui õiguskaitseasutus kavatseb näotuvastustehnoloogiat edasi arendada (õpetada), kehtivad arendusetapis õpetamis-, valideerimis- ja testimisandmetike ning arenduskeskkonna rollide/näitajate kohta lisanõuded. Kui valmistoode vajab kavandatud otstarbeks lisakohandusi, tuleks testimiseks, valideerimiseks ja õpetamiseks kasutatavate andmetike valikul järgida eespool mainitud lisanõudeid.

Samasse õiguskaitseasutusse kuulumine ei taga iseenesest täielikku juurdepääsu biomeetrilistele andmetele. Nagu mis tahes muude isikuandmete liikide puhul, ei saa biomeetrilisi andmeid, mida kogutakse teatud õiguskaitse eesmärgiks konkreetsel õiguslikul alusel, kasutada ilma nõuetekohase õigusliku aluseta muuks õiguskaitse eesmärgiks (direktiivi (EL) 2016/680 artikli 4 lõige 2). Kuivõrd näotuvastustehnoloogia vahendi arendamist/õpetamist peetakse erinevaks eesmärgiks, tuleks hinnata, kas biomeetriliste andmete töötlemine tulemuslikkuse mõõtmiseks / tehnoloogia õpetamiseks – et vältida mõju andmesubjektidele kehva tulemuslikkuse tõttu – on töötlemise esialgset eesmärki arvestades vajalik ja proportsionaalne.

1. ÜLESANDED JA KOHUSTUSED

Kui õiguskaitseasutus rakendab näotuvastustehnoloogiat, et täita õiguskaitse direktiivi kohaldamisalasse kuuluvaid ülesandeid (süütegude tõkestamine, uurimine, avastamine, nende eest vastutusele võtmine jne, nagu on sätestatud õiguskaitse direktiivi artiklis 3), võib teda pidada näotuvastustehnoloogia valdkonnas vastutavaks töötlejaks. Õiguskaitseasutused koosnevad aga mitmest üksusest/osakonnast, mis võivad osaleda selles töötlemises näotuvastustehnoloogia rakendusprotsessi määratlemise või praktikas kohaldamise kaudu. Selle tehnoloogia eripära tõttu võib olla vaja kaasata erinevaid üksusi, kes aitaksid mõõta vahendi tulemuslikkust või seda täiendavalt õpetada.

Õiguskaitseasutustes võib olla vaja kaasata näotuvastustehnoloogia projekti mitu sidusrühma⁷¹:

- Kõrgem juhtkond – kiidab projekti heaks pärast riskide ja võimaliku kasu kaalumist.
- Õiguskaitseasutuse andmekaitse spetsialist ja/või õigusosakond – aitab hinnata konkreetse näotuvastustehnoloogia projekti rakendamise õiguspärasust; abistab andmekaitsealase mõjuhinnangu tegemisel; tagab andmesubjektide õiguste austamise ja teostamise.

⁷⁰ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

⁷¹ Allpool kirjeldatud rollid kajastavad eri sidusrühmi ja nende vastutust näotuvastustehnoloogia projektis. Käesolevas lisas esitatud rollide kirjeldused ei ole lõplikud ning iga õiguskaitseasutus peab määratlema ja omistama sarnased rollid vastavalt oma organisatsiooni struktuurile. Võib juhtuda, et teatud üksus täidab rohkem kui üht rolli, näiteks protsessiomanik ja võrdlusandmebaasi haldur või protsessiomanik ja tehisintellekti ja/või andmeteaduse IT-osakond (kui protsessiomaniku üksuses on olemas kõik vajalikud tehnilised teadmised).

- Protsessiomanik – tegutseb pädeva õiguskaitseasutuse konkreetse üksusena projekti arendamisel; otsustab näotuvastustehnoloogia projekti üksikasjad, sh süsteemi tööõuded; kehtestab asjakohased õiglaste väärtuste parameetrid; määrab usaldusväärsuse skoori⁷²; kehtestab vastuvõetavad kallutatuse künnised; teeb kindlaks näotuvastustehnoloogia projekti võimalikud riskid üksikisikute õigustele ja vabadustele (konsulteerides ka andmekaitse spetsialisti ning tehisintellekti ja/või andmeteaduse IT-osakonnaga (vt allpool)) ning esitab need kõrgemale juhtkonnale. Protsessiomanik konsulteerib enne näotuvastustehnoloogia projekti üksikasjade üle otsustamist ka võrdlusandmebaasi halduriga, et tutvuda võrdlusandmebaasi kasutusotstarbe ja tehniliste üksikasjadega. Ostetud näotuvastustehnoloogia ümberõpetamise korral vastutab protsessiomanik ka õpetamisandmestiku valimise eest. Kuna protsessiomaniku ülesanne on projekti arendamine ja üksikasjade määratlemine, vastutab ta ka andmekaitsealase mõjuhinna tegemise eest.
- Tehisintellekti ja/või andmeteaduse IT-osakond – aitab koostada andmekaitsealase mõjuhinna; selgitab süsteemi toimimise, õigluse⁷³ ja võimaliku kallutatuse parameetreid; rakendab tehnoloogiat ja tehnilisi kaitsemeetmeid, et vältida loata juurdepääsu kogutud andmetele, küberründeid jne. Ostetud näotuvastustehnoloogia ümberõpetamise korral õpetab tehisintellekti või andmeteaduse IT-osakond süsteemi, tuginedes protsessiomaniku esitatud õppeandmestikule. See osakond kehtestab ka meetmed, mis aitavad leevendada protsessiomanike poolt ühiselt tuvastatud riske (nt tehisintellektile omased riskid, näiteks mudeli tuletamisega seotud rünnakud).
- Lõppkasutajad (nt politseiametnikud kohapeal või kohtuekspertiisilaborites) – teevad võrdluse andmebaasiga; vaatavad tulemusi kriitiliselt läbi, võttes arvesse varasemaid tõendeid, ja annavad tagasisidet protsessiomanikule valepositiivsete tulemuste ja võimaliku diskrimineerimise tunnuste kohta.
- Võrdlusandmebaasi haldur – pädeva õiguskaitseasutuse konkreetne üksus, kes vastutab võrdlusandmebaasi (st andmebaasi, millega kujutisi võrreldakse) koostamise ja haldamise, sealhulgas näokujutiste kustutamise eest pärast kindlaksmääratud säilitamisperioodi. Sellise andmebaasi võib luua spetsiaalselt kavandatava näotuvastustehnoloogia projekti jaoks või on see juba loodud sarnaseks otstarbeks. Võrdlusandmebaasi halduri ülesanne on määrata kindlaks, millal ja mis asjaoludel saab näokujutisi salvestada, ja kehtestada andmete säilitamise nõuded (aeg või muud kriteeriumid).

Kuna enamiku näotuvastustehnoloogia rakendamise ja kasutamise juhtumitega kaasneb olemuslikult suur risk andmesubjektide õigustele ja vabadustele, peaks olema kaasatud ka andmekaitse järelevalveasutus õiguskaitse direktiivi artiklis 28 nõutud eelneva konsulteerimise kontekstis.

2. ALGETAPP / ENNE NÄOTUVASTUSTEHNOLOOGIA SÜSTEEMI HANKIMIST

Õiguskaitseasutuses protsessi eest vastutaval omanikul peaks alustuseks olema selge arusaam näotuvastustehnoloogia kasutamise protsessi(de)st (kasutusjuhtum(id)) ning ta peaks tagama, et kavandatud kasutusjuhtumi põhjendamiseks oleks õiguslik alus. Sellele tuginedes peab ta tegema järgmist:

⁷² Usaldusväärsuse skoor on prognoosi (kokkulangevuse) usaldusnivoo, mis on väljendatud tõenäosusena. Näiteks kahe malli võrdlemisel on 90% tõenäosus, et need kuuluvad samale isikule. Usaldusväärsuse skoor on küll erinev näotuvastustehnoloogia tulemuslikkusest, kuid mõjutab seda. Mida kõrgem on näotuvastustehnoloogia usalduskünnis, seda vähem annab see valepositiivseid ja seda rohkem valenegatiivseid tulemusi.

⁷³ Õiglust võib määratleda kui ebaseadusliku diskrimineerimise, nt soolise või rassilise diskrimineerimise puudumist.

- Kasutusjuhtumi formaalne kirjeldus. Tuleb kirjeldada lahendamist vajavat probleemi ja seda, kuidas näotuvastustehnoloogia selle lahendab, andes ka ülevaate protsessist (ülesandest), mille raames tehnoloogiat rakendatakse. Sellega seoses peaksid õiguskaitseasutused dokumenteerima vähemalt järgmised elemendid⁷⁴:
 - Protsessis salvestatud isikuandmete liigid
 - Üldised ja konkreetsed eesmärgid, mille jaoks näotuvastustehnoloogiat kasutatakse, sealhulgas võimalikud tagajärjed andmesubjektile pärast kokkulangevust.
 - Millal ja kuidas näokujutisi kogutakse (sh kogumise kontekst, nt lennujaamaväravas, videod poe turvakaamerate, kus kuritegu sooritati jne, ning andmesubjektide kategooriad, kelle biomeetrilisi andmeid töödeldakse).
 - Andmebaas, millega pilte võrreldakse (võrdlusandmebaas), samuti teave selle loomise viisi, suuruse ja selles sisalduvate biomeetriliste andmete kvaliteedi kohta.
 - Õiguskaitseasutused, kellel on õigus kasutada näotuvastussüsteemi ja sellele tugineda õiguskaitse kontekstis (nende profiilid ja juurdepääsuõigused peab määrama protsessiomanik).
 - Sisendandmete kavandatud säilitamisaeg või ajahetk, mil see lõpeb (nt selle kriminaalmenetluse lõpetamine või lõppemine kooskõlas siseriikliku menetlusõigusega, mille jaoks andmed algselt koguti), samuti kõik järgnevad meetmed (andmete kustutamine, anonüümimine ja kasutamine statistika või teadusuuringute eesmärgil jne).
 - Logide pidamine ning logide ja säilitatavate dokumentide juurdepääsetavus.
 - Tulemuslikkuse näitajad (nt täpsus, mäletamisvõime, F1-skoor) ja nende vastuvõetavad miinimumkünnised.⁷⁵
 - Hinnang, kui paljudele isikutele näotuvastustehnoloogiat kohaldatakse ja mis ajavahemikul/olukorras.
- Vajalikkuse ja proportsionaalsuse hindamise läbiviimine⁷⁶. Asjaolu, et selline tehnoloogia on olemas, ei tohiks olla selle kasutamise ajendiks. Kõigepealt peab protsessiomanik hindama, kas kavandatud töötlemiseks on olemas asjakohane õiguslik alus. Selleks tuleb konsulteerida andmekaitse spetsialisti ja õigusteenistusega. Näotuvastustehnoloogia kasutuselevõtu peaks tingima asjaolu, et see on vajalik ja proportsionaalne lahendus õiguskaitseasutuste määratletud konkreetsele probleemile. Seda tuleks hinnata, võttes arvesse eesmärki / kuriteo raskusastet / mitteseotud isikute arvu, keda näotuvastussüsteem mõjutab. Õiguspärasuse hindamisel tuleks arvesse võtta vähemalt järgmist: Õiguskaitse direktiiv⁷⁷, isikuandmete kaitse üldmäärus^{78 79}, mis

⁷⁴ I lisas on esitatud loetelu elementidest, mis aitavad vastutaval töötlejal kirjeldada näotuvastustehnoloogia kasutusjuhtumit.

⁷⁵ Näotuvastustehnoloogia tulemuslikkuse hindamiseks on erinevaid parameetreid. Iga parameeter annab erineva ülevaate süsteemi tulemustest ning selle edukus näotuvastussüsteemi toimivuse kajastamisel sõltub näotuvastustehnoloogia kasutusjuhtumist. Kui soovitakse saavutada nägude korrektse kokkusobitamise kõrge protsent, võiks kasutada selliseid parameetreid nagu täpsus ja mäletamisvõime. Need parameetrid ei kajasta aga seda, kui hästi töötleb näotuvastustehnoloogia negatiivseid näiteid (kui palju oli valesti sobitatud nägusid). Protsessiomanik, keda toetab tehisintellekti ja andmeteaduse IT-osakond, peaks suutma kehtestada süsteemi tööõnõud ja väljendada neid sobivaimates parameetrites vastavalt näotuvastustehnoloogia kasutusjuhtumile.

⁷⁶ Vajadusel võib süsteemi kohandamine ja kasutamine nõuda lisameetmeid, mistõttu võib vajalikkuse ja proportsionaalsuse hindamise käigus ka kasutusjuhtumi kirjeldust veidi muuta.

⁷⁷ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil.

⁷⁸ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.

⁷⁹ Kui teadusprojekt, mille eesmärk on uurida näotuvastustehnoloogia kasutamist, peaks töötleva isikuandmeid, kuid selline töötlemine ei kuulu õiguskaitse direktiivi artikli 4 lõike 3 alla, kohaldatakse üldjuhul isikuandmete

tahes kehtiv tehisintellekti käsitlev õigusraamistik⁸⁰ ning kõik andmekaitse järelevalveasutuste esitatud täiendavad suunised (nt EDPB suunised 3/2019 isikuandmete töötlemise kohta videoseadmetes⁸¹). Neid ELi õigusakte tuleks alati toetada kohaldatavate siseriiklike nõuetega, eelkõige kriminaalmenetlusõiguse valdkonnas. Proportsionaalsuse hindamisel tuleks kindlaks teha andmesubjektide põhiõigused, mida see tehnoloogia võib mõjutada (lisaks eraelu puutumatusele ja andmekaitsele). Samuti tuleks kirjeldada ja kaaluda kõiki näotuvastustehnoloogia kasutusjuhtumi piiranguid (või piirangute puudumist). Näiteks, kas süsteem töötab pidevalt või ajutiselt ja kas see on piiratud kindla geograafilise piirkonnaga.

- Andmekaitsealase mõjuhinna koostamine⁸². Koostada tuleks andmekaitsealane mõjuhindang, sest näotuvastustehnoloogia kasutamisega õiguskaitse valdkonnas kaasneb suur risk üksikisikute õigustele ja vabadustele⁸³. Andmekaitsealane mõjuhindang peaks eelkõige sisaldama kavandatavate töötlemistoimingute üldist kirjeldust⁸⁴, andmesubjektide õigustele ja vabadustele avalduvate ohtude hinnangut⁸⁵, nende ohtude kõrvaldamiseks kavandatud meetmeid, kaitsemeetmeid, turvameetmeid ja -mehhanisme, et tagada isikuandmete kaitse ja tõendada nõuetele vastavust. Andmekaitsealane mõjuhindang on pidev protsess, mistõttu igas projekti etapis tuleks lisada kõik uued töötlemise elemendid ja ajakohastada riskihinnangut.
- Kõrgemalt juhtkonnalt nõusoleku küsimine, selgitades andmesubjektide õiguste ja vabadustele avalduvaid ohte (mis tulenevad kasutusjuhtumist ja tehnoloogiast) ning vastavaid riskide ennetamise kavasid.

3. NÄOTUVASTUSTEHTNOLOOGIA HANKEETAPIS JA ENNE KASUTUSELEVÕTTU

- Näotuvastustehnoloogia (algoritmi) valikukriteeriumide kindlaksmääramine. Protsessiomanik peaks tehisintellekti ja/või andmeteaduse IT-osakonna abiga otsustama algoritmi valimise kriteeriumid. Praktikas peaksid need hõlmama õigluse ja tulemuslikkuse parameetreid, mida on nimetatud kasutusjuhtumi kirjelduses. Need kriteeriumid peaksid sisaldama ka teavet andmetest, mille alusel algoritmi õpetati. Õpetamis-, testimis- ja valideerimisandmestik peab sisaldama

kaitse üldmäärust (õiguskaitse direktiivi artikli 9 lõige 2). Katseprojektides, millele järgnevad õiguskaitsetoimingud, oleks õiguskaitse direktiiv kohaldatav.

⁸⁰ Näiteks on esitatud ettepanek võtta vastu EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, MILLEGA NÄHAKSE ETTE TEHISINTELLEKTI KÄSITLEVAD ÜHTLUSTATUD ÕIGUSNORMID (TEHISINTELLEKTI KÄSITLEV ÕIGUSAKT) JA MUUDETAKSE TEATAVAID LIIDU ÕIGUSAKTE, kuid seda ei ole veel määrusena vastu võetud.

⁸¹https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

⁸² Lisasuunised andmekaitsealase mõjuhinna kohta on siin: Dokument WP248 rev.01 „Suunised, mis käsitlevad andmekaitsealast mõjuhinna ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena tõenäoliselt „tekib suur oht“ määruse 2016/679 tähenduses“, aadressil: <https://ec.europa.eu/newsroom/article29/items/611236>, ning Euroopa Andmekaitseinspektori kohapealse vastutuse vahendikomplekt, II osa, aadressil: https://edps.europa.eu/node/4582_en

⁸³ Näotuvastustehnoloogia võib sõltuvalt kasutusjuhtumist kuuluda järgmiste kriteeriumide alla, millest tuleneb suure riskiga töötlemine (andmekaitsealase mõjuhinna suunised, WP 248 rev.01): Süstemaatiline seire, suuremahuline andmetöötlus, andmetike sobitamine või ühendamine, uuenduslik kasutamine või uute tehnoloogiliste või korralduslike lahenduste rakendamine.

⁸⁴ Eespoolsetes etappides esitatud töötlemise kirjeldus ning vajalikkuse ja proportsionaalsuse hindamine on samuti osa andmekaitsealast mõjuhinna, v.a riskihindamine. Vajadusel esitatakse andmekaitsealases mõjuhinna isikuandmete voogude üksikasjalikum kirjeldus.

⁸⁵ Andmesubjektidele avalduvate riskide analüüs peaks hõlmama riske, mis tulenevad võrreldavate näokujutiste asukohast (kohapealne/kaugtöötlus), töötlejate/alltöötajatega seotud riske, samuti masinõppega (kui seda kasutatakse) seotud riske (nt andmemürgitus, konfliktid näited).

piisavalt valimeid nende andmesubjektide kõigist tunnustest, kellele näotuvastustehnoloogiat kohaldatakse (nt vanus, sugu ja rass), et vähendada süsteemi kallutatust. Näotuvastustehnoloogia teenuse osutaja peaks esitama selle tehnoloogia õpetamis-, testimis- ja valideerimisandmetike teabe ja parameetrid ning kirjeldama võimaliku ebaseadusliku diskrimineerimise ja kallutatuse mõõtmise ja leevendamise meetmeid. Protsessiomanik peab võimaluse korral kontrollima, kas teenuseosutajal oli õiguslik alus kasutada kõnealust andmestikku algoritmide õpetamiseks (teenuseosutaja poolt kättesaadavaks tehtud teabe põhjal). Samuti peaks protsessiomanik tagama, et näotuvastustehnoloogia teenuse osutaja kohaldab biomeetriliste andmetega seotud turvastandardeid, näiteks ISO/IEC 24745, mis annab juhiseid biomeetrilise teabe kaitseks vastavalt erinevatele konfidentsiaalsuse, tervikluse ja uuendatavuse/tühistatavuse nõuetele säilitamise ja edastamise ajal ning biomeetrilise teabe turvalisust ja privaatsust austava haldamise ja töötlemise nõuetele ja suunistele.

- Algoritmi ümberõpetamise korraldamine (vajaduse korral). Protsessiomanik peaks tagama, et näotuvastussüsteemi kasutuseelne seadistamine suurema täpsuse saavutamiseks kuuluks hangitud teenuste juurde. Kui täpsusparameetrite täitmiseks on vaja ostetud näotuvastussüsteemi lisakoolitust, peab protsessiomanik lisaks ümberõpetamise otsusele tehisintellekti ja/või andmeteaduse IT-osakonna abiga kindlaks määrama, millist sobivat ja representatiivset andmestikku kasutada, ning kontrollima andmete kasutamise seaduslikkust.
- Asjakohaste kaitsemeetmete kehtestamine turvalisuse, kallutatuse ja madala tulemuslikkusega seotud riskide käsitlemiseks. See hõlmab protsessi kehtestamist kasutusse võetud näotuvastustehnoloogia järelevalveks (logimine ja tagasiside tulemuste täpsuse ja õigluse tagamiseks). Lisaks tuleb tagada, et tuvastataks, mõõdetaks ja leevendataks teatavatele masinõppe ja näotuvastustehnoloogia süsteemidele omaseid riske (nt andmemürgitus, konfliktid näited, otsustusprotsessi läbipaistvusest tulenevad probleemid). Protsessiomanik peaks kehtestama ka asjakohased kaitsemeetmed, et tagada ümberõpetamise andmestikus sisalduvate biomeetriliste andmete säilitamise nõuete järgimine.
- Näotuvastussüsteemi dokumenteerimine. See peaks hõlmama näotuvastussüsteemi üldist kirjeldust, süsteemi elementide ja selle rakendamise protsessi üksikasjalikku kirjeldust, üksikasjalikku teavet näotuvastussüsteemi seire, toimimise ja juhtimise kohta ning üksikasjalikku kirjeldust selle riskide ja leevendusmeetmete kohta. Selle dokumentatsiooni elemendid hõlmavad näotuvastussüsteemi kirjelduse põhielemente eelmistest etappidest (vt eespool), kuid neid täiendatakse teabega, mis on seotud süsteemi tulemuslikkuse jälgimise ja muudatuste juurutamise, sh versioonide ajakohastamise ja/või ümberõpetamisega.
- Tehnoloogiat ja kasutusjuhtumeid selgitavate kasutusjuhendite koostamine. Kasutusjuhendites tuleb selgesõnaliselt selgitada kõiki stsenaariume ja eeltingimusi, mille alusel näotuvastustehnoloogiat kasutatakse.
- Lõppkasutajate õpetamine, kuidas tehnoloogiat kasutada. Nende koolituste käigus tuleks selgitada selle tehnoloogia võimalusi ja piiranguid, et kasutajad mõistaksid, mis asjaoludel saab seda kasutada ja mis juhtudel võib see olla ebatäpne. Need koolitused aitavad maandada ka riske, mis tulenevad algoritmi tulemuste vähesest kontrollimisest/kritiseerimisest.
- Andmekaitse järelevalveasutusega konsulteerimine vastavalt õiguskaitseDirektiivi artikli 28 lõike 1 punktile b. Teabe esitamine vastavalt õiguskaitseDirektiivi artiklile 13, et teavitada andmesubjekte töötlemisest ja nende õigustest. Need teated peavad olema suunatud andmesubjektidele sobivas keeles, et nad saaksid töötlemisest aru, ja selgitavad tehnoloogia põhielemente, sealhulgas täpsusmäärasid, õpetamisandmestikke ja meetmeid diskrimineerimise ja algoritmi kehva täpsuse ennetamiseks.

4. SOOVITUSED PÄRAST NÄOTUVASTUSTEHNOLOOGIA KASUTUSELEVÖTTU

- Inimsekkumise ja tulemuste järelevalve tagamine. Mitte kunagi ei tohi võtta vastu üksikisikuid puudutavaid otsuseid üksnes näotuvastustehnoloogia tulemuste põhjal (see tähendaks õiguskaitseinspektori artikli 11 rikkumist, st automatiseeritud töötusel põhinevate üksikotsuste tegemist, millel on andmesubjektile õiguslikud või muud sarnased tagajärjed). Tuleks tagada, et õiguskaitseasutuse ametnik vaatab näotuvastustehnoloogia tulemused läbi. Samuti tuleks tagada, et õiguskaitseasutustest kasutajad väldiksid kalduvust eelistada automatiseerimist, uurides vastuolulist teavet ja analüüsides tehnoloogia tulemusi kriitiliselt. Seetõttu on oluline lõppkasutajate jätkuv koolitamine ja teadlikkuse suurendamine, kuid kõrgem juhtkond peaks siiski tagama, et tööüha järelevalve teostamiseks on piisavalt inimressursse. See tähendab, et igale ametnikule antakse tehnoloogia tulemuste kriitiliseks analüüsimiseks piisavalt aega. Tuleks dokumenteerida, mõõta ja hinnata, mil määral inimjärelevalve muudab näotuvastustehnoloogia poolt tehtud esialgset otsust.
- Näotuvastustehnoloogia mudeli hälbe (tulemuslikkuse halvenemise) seire ja haldamine, kui mudel on kasutusele võetud.
- Protsessi kehtestamine riskide ja turvameetmete ümberhindamiseks teatava ajavahemiku tagant või kui tehnoloogia või selle kasutusjuhtum muutub.
- Kõigi süsteemi muudatuste dokumenteerimine kogu selle olelusringi jooksul (nt uuendused, ümberõpetamine).
- Protsessi ja tehnilise suutlikkuse loomine, et hallata andmesubjektide andmetega tutvumise taotlusi. Enne mis tahes taotluse vastuvõtmist peab olema loodud tehniline suutlikkus andmete väljavõtete tegemiseks juhul, kui andmesubjektid neid taotleavad.
- Andmerikkumiste käsitlemise korra tagamine. Kui toimub isikuandmetega seotud rikkumine, mis hõlmab biomeetrilisi andmeid, on riskid tõenäoliselt suured. Sellisel juhul peaksid kõik puudutatud kasutajad olema teadlikud korrast, mida tuleb järgida, ning viivitamata tuleks teavitada ka andmekaitseinspektori ja andmesubjekte.

III LISA. PRAKTILISED NÄITED

Näotuvastust kasutatakse paljudes erinevates olukordades ja eesmärkidel, näiteks kontrollitud keskkondades, nagu piiriületused, ristkontroll politseiandmebaasidest saadud andmetega või andmesubjekti poolt ilmselt avalikustatud isikuandmetega, reaalajas andmeid edastavad kaamerad (reaalajas näotuvastus) jne. Sellepärast on isikuandmete ning muude põhiõiguste ja -vabaduste kaitsega seotud riskid erinevatel kasutusjuhtudel väga erinevad. Et hõlbustada vajalikkuse ja proportsionaalsuse hindamist, mis peaks eelnema otsuse tegemisele näotuvastustehnoloogia võimaliku kasutamise kohta, esitatakse neis suunistes mittetäielik loetelu näotuvastustehnoloogia võimalikest rakendustest õiguskaitse valdkonnas.

Siin esitatud ja hinnatud stsenaariumid põhinevad **hüpoteetilistel** olukordadel ning nende eesmärk on näitlikustada teatud konkreetseid näotuvastustehnoloogia kasutusviise, pakkuda abi juhtumipõhiste kaalutlustega ning kehtestada üldine raamistik. Stsenaariumid ei ole ammendavad ja ei piira ühtegi käimasolevat või tulevast menetlust, mille siseriiklik järelevalveasutus algatab seoses näotuvastustehnoloogiatega väljatöötamise, katsetamise või rakendamisega. Nende stsenaariumide eesmärk on üksnes näitlikustada selles dokumendis esitatud suuniseid poliitikakujundajatele, seadusandjatele ja õiguskaitseasutustele, kes näotuvastustehnoloogia rakendamist kaaluvad ja kavandavad, et tagada täielik vastavus ELi õigustikule isikuandmete kaitse valdkonnas. Sellega seoses tuleb mees pidada, et isegi sarnastes näotuvastustehnoloogia kasutamise olukordades võib teatavate elementide olemasolu või puudumine anda vajalikkuse ja proportsionaalsuse hindamisel teistsuguse tulemuse.

1 1. STSENAARIUM

1.1. Kirjeldus

Automatiseeritud piirikontrollisüsteem, mis võimaldab automaatset piiriületust, autentides ELi kodanike ja teiste piiripunkti läbivate reisijate elektroonilises reisidokumendis salvestatud biomeetrilise kujutise ja tehes kindlaks, et reisija on dokumendi seaduslik omanik.

Selline kontrollimine/autentimine hõlmab ainult üks-ühele näotuvastust ja seda tehakse kontrollitud keskkonnas (nt lennujaamade e-väravates). Piiripunkti läbiva reisija biomeetrilised andmed salvestatakse, kui talle antakse selgesõnaline käsk vaadata e-värava kaamerasse, ja neid võrreldakse esitatud dokumendi (pass, ID-kaart jne) andmetega, mis on väljastatud kooskõlas konkreetsete tehniliste nõuetega.

Ehkki töötlemine jääb sellistel juhtudel põhimõtteliselt õiguskaitse direktiivi kohaldamisalast välja, võib kontrolli tulemust kasutada ka isiku (tähtnumbriliste) andmete võrdlemiseks õiguskaitseandmebaasidega piirikontrolli raames ning seega võib see hõlmata andmesubjekti jaoks olulise õigusliku tagajärjega meetmeid, näiteks vahistamist Schengeni infosüsteemi (SIS) hoiatusteate alusel. Teatavatel asjaoludel võib biomeetrilisi andmeid kasutada ka õiguskaitseasutuste andmebaasidest kokkulangevuste otsimiseks (sellisel juhul toimub selles etapis üks-ühele tuvastamine).

Biomeetrilise kujutise töötlemise tulemus mõjutab otseselt andmesubjekti: ta võib piiri ületada üksnes siis, kui kontroll on edukas. Kui isiku tuvastamine ebaõnnestub, peavad piirivalveametnikud tegema teise kontrolli, et veenduda, et andmesubjekt erineb isikut tõendavas dokumendis esitatust.

Kui tuvastatakse Schengeni infosüsteemi (SISi) või riiklik hoiatusteade, peavad piirivalveametnikud tegema teise kontrolli ja järgnevad vajalikud lisakontrollid ning seejärel võtma vajalikke meetmeid, nt vahistama isiku, teavitama asjaomaseid asutusi.

Teabe allikas

- Andmesubjektide liigid: ☒ kõik piiri ületavad isikud
- Kujutise allikas: ☒ muu (isikut tõendav dokument)
- Seos kuritegevusega: ☒ ei ole vajalik
- Teabe kogumise viis: ☒ kabiinis või kontrollitud keskkonnas
- Kontekst – mõjutab teisi põhiõigusi: jah, nimelt: ☒ vaba liikumise õigus ☒ varjupaigaõigus

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☒ piirikontrolliga seotud erandmebaasid

Algoritm

- Kontrolli liik: ☒ üks-ühele kontroll (autentimine)

Tulemus

- Mõju ☒ otsene (andmesubjektil lubatakse või ei lubata riiki siseneda)
- Automatiseeritud töötlusel põhinev otsus: ☒ jah

1.2. Kohaldatav õigusraamistik

Alates 2004. aastast peavad liikmesriikide väljastatud passid ja muud reisidokumendid vastavalt nõukogu määrusele (EÜ) nr 2252/2004⁸⁶ sisaldama biomeetrilist näokujutist, mis on salvestatud dokumendis sisalduvale elektroonilisele kiibile.

Schengeni piirieeskirjades⁸⁷ on sätestatud nõuded isikute kontrollimiseks välispiiridel. ELi kodanike ja teiste liidu õiguse alusel vaba liikumise õigust kasutavate isikute puhul peaks minimaalne kontroll hõlmama nende reisidokumentide kontrollimist, kasutades vajadusel tehnilisi vahendeid. Schengeni piirieeskirju on muudetud määrusega (EL) 2017/2225⁸⁸, millega kehtestati muu hulgas mõistete „e-värvavad“, „automaatne piirikontrollisüsteem“ ja „iseteenindussüsteem“ määratlused ning võimalus töödelda biomeetrilisi andmeid piirikontrolli käigus.

Seega võib eeldada, et on olemas selge ja ettenähtav õiguslik alus, mis lubab sellist isikuandmete töötlemist. Lisaks on õigusraamistik vastu võetud liidu tasandil ja see on liikmesriikidele vahetult kohaldatav.

1.3. Vajalikkus ja proportsionaalsus – kuriteo eesmärk/raskusaste

ELi kodanike isikusamasuse kontrollimine automaatse piirikontrolli käigus, kasutades nende biomeetrilist kujutist, on osa ELi välispiiridel tehtavast piirikontrollist. Järelikult on see otseselt seotud piirijulgeolekuga ja teenib liidu poolt tunnustatud üldist huvi pakkuvat eesmärki. Lisaks aitavad automaatse piirikontrolli värvavad kiirendada reisijate töötlemist ja vähendada inimlike eksimuste riski. Peale selle on sekkumise ulatus ja intensiivsus selle stsenaariumi korral palju piiratunud kui muud näotuvastuse viisid. Siiski tekitab biomeetriliste andmete töötlemine andmesubjektidele lisariske,

⁸⁶ NÕUKOGU MÄÄRUS (EÜ) nr 2252/2004, 13. detsember 2004, liikmesriikide poolt väljastatud passide ja reisidokumentide turvaelementide ja biomeetria standardite kohta.

⁸⁷ EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 2016/399, 9. märtsi 2016, mis käsitleb isikute üle piiri liikumist reguleerivaid liidu eeskirju (Schengeni piirieeskirjad).

⁸⁸ Euroopa Parlamendi ja nõukogu määrus (EL) 2017/2225, 30. november 2017, millega muudetakse määrust (EL) 2016/399 riiki sisenemise ja riigist lahkumise süsteemi kasutamise osas.

mida peab näotuvastustehnoloogiat rakendav ja opereeriv pädev asutus nõuetekohaselt käsitlema ja leevendama.

1.4. Järeldus

ELi kodanike isikusamasuse kontrollimine automatiseeritud piirikontrolli kontekstis on vajalik ja proportsionaalne meede, kui on kehtestatud asjakohased kaitsemeetmed, eelkõige eesmärgi piiritlemise, andmete kvaliteedi, läbipaistvuse ja turvalisuse kõrge taseme põhimõtete kohaldamise kaudu.

2 2. STSENAARIUM

2.1. Kirjeldus

Õiguskaitseasutused kehtestavad lapseröövi ohvrite tuvastamise süsteemi. Volitatud politseiametnik võib rangetel tingimustel võrrelda lapseröövi kahtlusega lapse biomeetrilisi andmeid lapseröövi ohvrite andmebaasiga, et tuvastada alaealised, kes võiksid vastata kadunud lapse kirjeldusele, kelle kohta on algatatud uurimine ja välja antud hoiatusteade.

Andmete töötlemine seisneb kadunud lapse kirjeldusele vastava isiku näo või pildi võrdlemises andmebaasis salvestatud piltidega. Selline töötlemine toimuks konkreetsetel juhtudel ja mitte süstemaatiliselt.

Võrdlusandmebaas sisaldab pilte kadunud lastest, kellega seoses on teatatud lapseröövi kahtlusest, lapse elu või füüsilise puutumatuse ohust ja on algatatud kohtuasutuses kriminaaluurimine ning kelle kohta on väljastatud lapserööviga seotud hoiatusteade. Andmeid kogutakse pädeva õiguskaitseasutuse kehtestatud menetluste raames, mida teostavad õiguskaitsealaste politseimissioonide volitustega politseiametnikud. Registreeritavad isikuandmete liigid on järgmised:

- identiteet, hüüdnimi, varjunimi, põlvnemine, kodakondsus, aadressid, e-posti aadressid, telefoninumbrid;
- sünniaeg ja -koht;
- teave põlvnemissuhte kohta;
- foto, mille tehnilised omadused võimaldavad kasutada näotuvastusseadet, ja muud fotod.

Võrdlustulemused peab läbi vaatama ja kontrollima volitatud ametnik, et kinnitada varasemaid tõendeid võrdlustulemuste alusel ja välistada võimalikud valepositiivsed tulemused.

Laste pilte ja isikuandmeid võib säilitada ainult hoiatusteate kestuse jooksul. Need tuleb kustutada kohe pärast kriminaalmenetluse lõppu kooskõlas riikliku menetlusega, mille jaoks need andmebaasi sisestati.

Ehkki biomeetriliste andmete säilitamisperiood andmebaasis võib olla suhteliselt pikk ja määratletud vastavalt siseriiklikule õigusele, annab andmesubjekti õiguste teostamine, eelkõige andmete parandamise ja kustutamise õigus lisatagatise, mis aitab piirata puudutatud andmesubjektide isikuandmete kaitse õigusesse sekkumist.

Teabe allikas

- Andmesubjektide liigid: ☒ lapsed

- Kujutise allikas ☒ muu: ei ole eelnevalt määratletud, kahtlustatav lapseröövi ohver
- Seos kuritegevusega ☒ otsene ajaline seos puudub ☒ otsene geograafiline seos puudub
- Teabe kogumise viis: ☒ kabiinis või kontrollitud keskkonnas
- Kontekst: mõjutab teisi põhiõigusi ☒ jah, nimelt: ☒ mitmed õigused

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus ☒ erandmebaas

Algoritm

- Kontrolli liik: ☒ üks-mitmele kontroll (identifitseerimine)

Tulemus

- Mõju ☒ otsene
- Automatiseeritud töötlusel põhinev otsus: ☒ EI, kohustuslik läbivaatamine volitatud ametniku poolt

Õiguslik analüüs

- Kohaldatav õigusraamistik: ☒ kõnealuse töötlemise suhtes kohaldatav spetsiifiline siseriiklik õigus (näotuvastus)

2.2. Kohaldatav õigusraamistik

Siseriiklikes õigusaktides on sätestatud eriõigusraamistik, mille alusel luuakse andmebaas, määratakse kindlaks töötlemise eesmärgid ning andmebaasi koostamise, juurdepääsu ja kasutamise kriteeriumid. Selle rakendamiseks vajalikud seadusandlikud meetmed näevad ette ka säilitamisaja kehtestamise ning viitavad kohaldatavatele tervikluse ja konfidentsiaalsuse põhimõtetele. Seadusandlikud meetmed näevad ette ka andmesubjektile ja antud juhul vanemliku vastutuse kandja(te)le teabe edastamise korra, samuti andmesubjekti õiguste kasutamise ja vajadusel nende võimaliku piiramise. Vastava seadusandliku meetme ettepaneku ettevalmistamisel tuli konsulteerida riikliku järelevalveasutusega.

2.3. Vajalikkus ja proportsionaalsus – kuriteo eesmärk / raskusaste / mitteseotud isikute arv, keda töötlemine mõjutab

Töötlemise tingimused ja kaitsemeetmed

Näotuvastusel põhinevat võrdlemist võib läbi viia üksnes volitatud ametnik viimase abinõuna, kui puuduvad muud vähem sekkuvad vahendid ja kui see on rangelt vajalik; näiteks juhul, kui kaheldakse reisisa alaealise isikut tõendava dokumendi autentsuses ja/või kui on läbi vaadatud varasemad tõendid ja materjalid, mis viitavad võimalikule vastavusele kadunud lapse kirjeldusega, kelle suhtes on juba algatatud kriminaaluurimine.

Täiendavaks kaitsemeetmeks on ka näotuvastusel põhineva võrdlemise kohustuslik läbivaatamine ja kontrollimine volitatud ametniku poolt, et kinnitada varasemaid tõendeid võrdlustulemuste alusel ja välistada võimalikud valepositiivsed tulemused.

Taotletav eesmärk

Andmebaasi loomine teenib üldise avaliku huviga seotud olulisi eesmärke, eelkõige kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist või kriminaalkaristuste täitmisele pööramist ning teiste isikute õiguste ja vabaduste kaitset. Andmebaasi loomine ja ettenähtav töötlemine aitavad eeldatavalt kaasa lapseröövi ohvriks langenud laste tuvastamisele ning seetõttu võib neid pidada sobivaks meetmeks, mis toetab õiguspärast eesmärki, st selliste kuritegude uurimist ja nende eest vastutusele võtmist.

Andmebaasi eesmärk ja selle koostamine

Töötlemise eesmärgid on seadusega selgelt määratletud ning andmebaasi kasutatakse üksnes selliste kadunud laste tuvastamiseks, kellega seoses on teatatud lapseröövi kahtlusest ja algatatud kohtuasutuse järelevalve all kriminaaluurimine ning kelle kohta on väljastatud lapseröövi hoiatustead. Andmebaasi koostamise seaduslike tingimuste eesmärk on rangelt piirata andmebaasi lisatavate andmesubjektide ja isikuandmete hulka. Vanemliku vastutuse kandjat tuleb teavitada käimasolevast töötlemisest ja lapse õiguste kasutamise tingimustest seoses isikutuvastuse eesmärgil töödeldavate biomeetriliste andmetega või andmebaasis säilitatavate laste isikuandmetega.

2.4. Järeldus

Võttes arvesse kavandatava töötlemise vajalikkust ja proportsionaalsust ning lapse parimaid huve sellisel isikuandmete töötlemisel ning kui on olemas piisavad tagatised, mis tagavad eelkõige andmesubjekti õiguste kasutamise – arvestades eriti asjaolu, et töödeldakse laste andmeid –, võib sellist näotuvastustehnoloogia kohaldamist pidada tõenäoliselt ELi õigusega kooskõlas olevaks.

Lisaks, arvestades töötlemise liiki ja kasutatavat tehnoloogiat, millega kaasneb suur risk puudutatud andmesubjekti õigustele ja vabadustele, leiab EDPB, et kavandatud töötlemisega seotud seadusandliku meetme ettepaneku või sellisel seadusandlikul meetmel põhineva reguleeriva meetme ettevalmistamine peab hõlmama eelnevat konsulteerimist järelevalveasutusega, et tagada järjepidevus ja vastavus kohaldatava õigusraamistikuga, vt õiguskaitse direktiivi artikli 28 lõiget 2.

3 3. STSENAARIUM

3.1. Kirjeldus

Rahutuste ajal toimunud politsei sekkumise ja hilisema uurimise käigus tuvastati mitmed isikud kahtlusallustena, tuginedes nt. varasemate uurimiste, videovalveseadmete salvestustele või tunnistajate ütlustele. Kahtlusalluste kujutisi võrreldakse isikute kujutistega, mis olid jäädvustatud videovalve- või mobiilseadmetesse kuriteopaigas või selle ümbruses.

Et saada üksikasjalikumaid tõendeid isikute kohta, keda kahtlustatakse meelevaieldusele järgnenud rahutustes osalemises, loob politsei andmebaasi, milles on rahutustega asukohaliselt ja ajaliselt enam-vähem seotud pildimaterjal. Andmebaas sisaldab kodanike poolt politseile saadetud isiklike salvestisi, ühistranspordi videokaamerate materjali, politseile kuuluvat videovalvematerjali ja piirangute või kaitsemeetmeteta avaldatud meediamaterjali. Andmebaasi failide lisamise eeltingimus ei ole ilmselgelt kuritegeliku käitumise ilming. Seetõttu talletatakse andmebaasis isikud, kes ei osalenud rahutustes – suur osa kohalikest elanikest, kes meelevaieldusest toimumise ajal mööda jalutasid või osalesid küll meelevaieldusel, kuid mitte rahutustes. Tegemist on tuhandete video- ja pildifailidega.

Näotuvastustarkvara abil määratakse kõikidele failides leiduvatele nägudele kordumatud näo identifikaatorid. Seejärel võrreldakse kahtlusalluste nägusid automaattöötluse teel nende näo identifikaatoritega. Tuhandetest video- ja pildifailidest saadud biomeetrilistest mallidest koostatud andmebaasi säilitatakse kuni kõigi võimalike uurimiste lõpuni. Positiivseid kokkulangevusi uurivad asjaga tegelevad ametnikud, kes otsustavad edasiste meetmete üle. See võib hõlmata andmebaasis sisalduva faili lisamist vastava isiku kriminaaltoimikusse, samuti lisameetmeid, näiteks isiku küsitlemist või vahistamist.

Siseriiklik õigus näeb ette üldise sätte, mille kohaselt on biomeetriliste andmete töötlemine füüsilise isiku kordumatu tuvastamise eesmärgil lubatud, kui see on rangelt vajalik ning puudutatud isiku õiguste ja vabaduste tagamiseks on kehtestatud asjakohased kaitsemeetmed.

Teabe allikas

- Andmesubjektide liigid: ☒ kõik isikud
- Kujutise allikas: ☒ avalikud kohad ☒ eraõiguslik üksus ☒ muud isikud ☒ muu: meedia
- Seos kuritegevusega: ☒ ei pea tingimata olema otsene geograafiline või ajaline seos
- Teabe kogumise viis: ☒ kaugmeetod
- Kontekst – mõjutab teisi põhiõigusi: jah, nimelt ☒ kogunemisvabaduse kontekstis
- Andmesubjektiga seotud kättesaadavad lisateabeallikad:
☒ muu: ei ole välistatud (nt sularahaautomaatide või kaupluste kaamerate kasutamine), sest kujutistega seotud motiive ei saa kontrollida

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☒ kuritegevuse valdkonnaga seotud eriandmebaasid

Algoritm

- Töötlemise viis: ☒ üks-mitmele tuvastamine

Tulemus

- Mõju: ☒ otsene (nt andmesubjekt võidakse vahistada, teda võidakse küsitleda)
- Automatiseeritud töötlusel põhinev otsus: ☒ EI
- Säilitamise kestus: kuni kõigi võimalike uurimiste lõpuni

Õiguslik analüüs

- Andmesubjektile eelnevalt antava teabe liik: ☒ üldteave õiguskaitseasutuse veebilehel
- Kohaldatav õigusraamistik: ☒ valdavalt siseriiklikku õigusesse ülevõetud õiguskaitseidirektiiv ☒ üldine siseriiklik õigus, mis käsitleb biomeetriliste andmete kasutamist õiguskaitseasutuste poolt

3.2. Kohaldatav õigusraamistik

Nagu eespool selgitatud, ei ole õiguskaitseidirektiivi artiklit 10 pelgalt kordavad õiguslikud alused piisavalt selged, et anda üksikisikutele adekvaatset teavet, mis tingimustel ja asjaoludel on õiguskaitseasutustel õigus kasutada avalikes kohtades tehtud videovalveseadmete salvestisi, et luua nende näo biomeetriline mall ja võrrelda seda politseiandmebaaside, muude olemasolevate videovalveseadmete või eraisikute salvestistega jne. Seega ei vasta käesolevas stsenaariumis mainitud õigusraamistik miinimumnõuetele, et seda saaks kasutada õigusliku alusena.

3.3. Vajalikkus ja proportsionaalsus

Selles näites tekitab töötlemine vajalikkuse ja proportsionaalsuse põhimõttest lähtuvalt mitmeid probleeme:

Isikuid ei kahtlustata raskes kuriteos. Ilmselt kuritegeliku käitumise ilming ei ole pildimaterjali sisaldava andmebaasi failide kasutamise eeltingimus. Samuti ei ole andmebaasi failide kasutamise eeltingimus otsene ajaline ja geograafiline seos kuriteoga. Selle tulemusena säilitatakse suure osa kohalike elanike andmeid biomeetrilises andmebaasis potentsiaalselt mitut aastat, kuni kõik uurimised on lõppenud.

Kuriteokoha andmebaas ei sisalda üksnes proportsionaalsusnõuetele vastavaid kujutisi, mistõttu on võrreldavate piltide hulk piiramatult suur. See on vastuolus võimalikult vähesete andmete kogumise

põhimõttega. Väiksem kujutiste hulk võimaldaks kaaluda ka mittealgoritmilisi ja vähem sekkuvaid meetmeid, nt näotuvastuseksperite.⁸⁹

Kuna näide pärineb rahvarahutustest, on tõenäoline, et kujutised paljastavad ka meeleavaldusel osalenute poliitilised veendumused, mis on selles stsenaariumis teine potentsiaalselt mõjutatud andmete eriliik. Selle stsenaariumi korral on ebaselge, kuidas ja mis meetmetega saaks nende andmete kogumist vältida. Lisaks, kui andmesubjektid saavad teada, et nad kanti meeleavaldusel osalemise järel politsei biomeetrilisse andmebaasi, võib see avaldada edaspidi olulist heidutavat mõju kogunemisõiguse kasutamisele.

Andmebaasis sisalduvaid biomeetrilisi malle saab samuti üksteisega võrrelda. See võimaldab politseil mitte üksnes otsida kogu salvestatud materjalist konkreetset isikut, vaid ka taastada isiku käitumismuster mitme päeva jooksul. Samuti võib see anda isikute, näiteks nende sotsiaalsete kontaktide ja poliitilise osaluse kohta lisateavet.

Sekkumist võimendab veelgi asjaolu, et andmeid töödeldakse andmesubjektide teadmata.

Kuna inimesed salvestavad fotosid ja videoid kogu aeg ning isegi kogu videoalvematerjali saab analüüsida biomeetriliselt, võib see avaldada tugevalt heidutavat mõju.

Teine probleemne aspekt on erafotode ja -videote laialdane kasutamine, sealhulgas võimalik väärkasutus, näiteks üldsuse hukkamõist. Kuivõrd väärkasutus, nagu üldsuse hukkamõist, on samuti kriminaalmenetlusele üldiselt omane risk, on see oluliselt suurem töödeldavate andmete skaleeritavuse ja seotud isikute arvu tõttu, sest inimesed võivad üles laadida ka materjali, mis on seotud konkreetse taunitava isiku või isikute rühmaga. Politsei üleskutse laadida üles fotosid ja videosid võib viia materjali esitamisel väga madala künniseni, eriti kui inimesed saavad seda teha anonüümselt või ilma et oleks vaja end politseiosakonnas identifitseerida.

3.4. Järeldus

Selles näites ei ole ühtegi erisätet, mis võiks olla õiguslikuks aluseks. Ent isegi kui õiguslik alus oleks piisav, ei oleks vajalikkuse ja proportsionaalsuse nõuded täidetud, mistõttu oleks tegemist ebaproportsionaalse sekkumisega andmesubjektide õigustesse eraelu puutumatusele ja isikuandmete kaitsele, mis on sätestatud hartas.

4 4. STSENAARIUM

4.1. Kirjeldus

Politsei võtab kasutusele viisi, kuidas tagasiulatuvalt näotuvastustehnoloogia abil tuvastada kahtluselused, kes on pannud toime videoalveseadmele salvestatud raske kuriteo. Ohvitser valib käsitsi kuriteopaigal või mujal eeluurimise käigus kogutud videomaterjalist saadud kahtluseluste pildi(d) ja saadab need kohtuekspertiisiosakonnale. Kohtuekspertiisiosakond kasutab näotuvastustehnoloogiat, et viia pildid vastavusse isikutega, kelle kujutised sisalduvad varasemas politseiandmebaasis (nn kirjeldav andmebaas, milles on kahtlustatavad ja endised süüdimõistatud). Kirjeldavat andmebaasi analüüsitakse selle menetluse jaoks – ajutiselt ja isoleeritud keskkonnas – näotuvastustehnoloogia abil, et kujutisi omavahel sobitada. Sobitatud isikute õigustesse ja huvidesse sekkumise vähendamiseks on kohtuekspertiisiosakonna väga vähestel töötajatel volitus

⁸⁹ Need on inimesed, kellel on erakordne nägude tuvastamise võime. Vt ka: Face Recognition by Metropolitan Police Super-Recogners, 2016 Feb 26, DOI: 10.1371/journal.pone.0150036, <https://pubmed.ncbi.nlm.nih.gov/26918457/>.

sobitusmenetluse läbiviimiseks ning andmetele on juurdepääs vaid ametnikel, kellele on usaldatud konkreetne toimik, ja enne iga tulemuse edastamist uurivale ametnikule toimub tulemuste käsitsi kontroll. Biomeetrilisi andmeid ei edastata väljaspoole kontrollitud, isoleeritud keskkonda. Edasises uurimises kasutatakse üksnes tulemust ja pilti (mitte biomeetrilist malli). Töötajad saavad isikuandmete töötlemise eeskirjade ja menetluste kohta erikoolituse ning igasugune isikuandmete ja biomeetriliste andmete töötlemine on liikmesriigi õiguses ammendavalt sätestatud.

Teabe allikas

- Andmesubjektide liigid: ☒ videovalveseadmete salvestiste põhjal tuvastatud kahtlusalused
- Kujutise allikas: ☒ avalikud kohad ☒ internet
- Seos kuritegevusega: ☒ otsene ajaline seos
☒ otsene geograafiline seos
- Teabe kogumise viis: ☒ kaugmeetod
- Kontekst – mõjutab teisi põhiõigusi: jah, nimelt: ☒ kogunemisvabadus ☒ sõnavabadus ☒ muud õigused: __

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☒ kuritegevuse valdkonnaga seotud eriandmebaasid

Algoritm

- Töötlemise viis: ☒ üks-mitmele tuvastamine

Tulemus

- Mõju: ☒ otsene (nt andmesubjekt vahistatakse, teda küsitletakse)
- Automatiseeritud töötlusel põhinev otsus: ☒ EI

Õiguslik analüüs

- Kohaldatav õigusraamistik: ☒ selles pädevas asutuses kõnealust töötlemist (näotuvastus) käsitlevad konkreetsed siseriiklikud õigusaktid

4.2. Kohaldatav õigusraamistik

Selle stsenaariumi korral on liikmesriigi õiguses sätestatud, et biomeetrilisi andmeid võib kasutada kohtuekspertiisis, kui see on rangelt vajalik, et saavutada raske kuriteo toime pannud kahtlusaluste tuvastamise eesmärk, sobitades kirjeldavas andmebaasis olevaid kujutisi. Siseriiklikus õiguses on sätestatud, milliseid andmeid tohib töödelda, samuti menetlused isikuandmete tervikluse ja konfidentsiaalsuse tagamiseks ning andmete hävitamiseks, et tagada piisav kaitse kuritarvituse ja omavoli riski vastu.

4.3. Vajalikkus ja proportsionaalsus

Näotuvastuse kasutamine on kohtuekspertiisi tasandil ilmselgelt ajatõhusam kui kujutiste käsitsi sobitamine. Kujutiste eelnev käsitsi valimine piirab sekkumist erinevalt kogu videomaterjali võrdlemisest andmebaasiga ning eristab seeläbi ainult isikud, kes jäävad eesmärgi, st raskete kuritegude vastase võitluse kohaldamisalasse. Sellegipoolest on oluline kaaluda, kas sobitamist saaks teha käsitsi mõistliku aja jooksul, olenevalt konkreetsest juhtumist. Tehnoloogiale ja isikuandmetele juurdepääsu saavate isikute arvu piiramine vähendab mõju eraelu puutumatuse ja andmekaitse õigustele ning biomeetrilistele mallidele, mida ei säilitata ega kasutata hilisema uurimise käigus. Tulemuste käsitsi kontroll tähendab ka valepositiivsete tulemuste riski vähenemist.

4.4. Järeldus

On oluline, et siseriiklikud õigusaktid tagaksid piisava õigusliku aluse biomeetriliste andmete töötlemise ja riikliku andmebaasi jaoks, millega neid andmeid sobitatakse. Selle stsenaariumi korral on kehtestatud mitu meetet, et piirata sekkumist andmekaitseõigustesse, näiteks õiguslikus aluses määratletud näotuvastustehnoloogia kasutamise tingimused, tehnoloogiale ja biomeetrilistele andmetele juurdepääsu omavate isikute arv, käsitsi kontroll jne. Näotuvastustehnoloogia parandab oluliselt politsei kohtuekspertiisiosakonna uurimistöö tõhusust ning põhineb seadusel, mis võimaldab politseil töödelda biomeetrilisi andmeid, kui see on hädavajalik, ja seetõttu võib seda nendes piirides pidada seaduslikuks sekkumiseks üksikisiku õigustesse.

5 5. STSENAARIUM

5.1. Kirjeldus

Biomeetriline kaugtuvastus tähendab seda, et isikute identiteet tuvastatakse biomeetriliste tunnuste (näokujutis, kõnnak, iiris jne) alusel distantstilt, avalikus kohas ja pideval või jooksva viisil, kontrollides neid tunnuseid andmebaasi salvestatud (biomeetriliste) andmetega⁹⁰. Biomeetriline kaugtuvastus toimub reaajas, kui pildimaterjali salvestamine, võrdlemine ja tuvastamine toimuvad märkimisväärse viivitusega.

Enne reaajas biomeetrilist kaugtuvastust koostab politsei uurimise seisukohast huvipakkuvate isikute jälgimisnimekirja. Nimekirja lisatakse isikute näokujutised. Tuginedes jälitusteabele, mis viitab sellele, et isikud asuvad konkreetsetes piirkonnas, näiteks ostukeskuses või avalikul väljakul, otsustab politsei, millal, kus ja kui kaua biomeetrilist kaugtuvastust rakendada.

Operatsioonipäeval pargitakse kohapeale juhtimiskeskusena toimiv politseikaubik, milles viibib vanem-politseiametnik. Kaubikus on kuvarid, millel kuvatakse salvestusmaterjal lähedal asuvatest ajutistest videovalvekaamerate või statsionaarsete kaamerate videovoogudest. Kui jalakäijad mööduvad kaamerate, hõivab tehnoloogia näokujutised, teisendab need biomeetriliseks malliks ja võrdleb neid jälgimisnimekirjas olevate isikute biomeetriliste mallidega.

Kui tuvastatakse jälgimisnimekirja ja kaamerate mööduvate isikute potentsiaalne kokkulangevus, saadetakse hoiatus sõidukis viibivatele ametnikele, kes teavitavad positiivset teadet kohapeal viibivaid ametnikke, nt raadioseadme kaudu. Kohapeal viibiv ametnik otsustab seejärel, kas sekkuda, läheneda või isik hoopis kinni pidada. Politseiametniku poolt kohapeal võetud meetmed dokumenteeritakse. Varjatud kontrolli korral salvestatakse kogutud teave (nt kellega isik aega veedab, mis rõivaid kannab ja kuhu suundub).

Osutatud siseriiklik õigus näeb ette üldise sätte, mille kohaselt on biomeetriliste andmete töötlemine füüsilise isiku kordumatu tuvastamise eesmärgil lubatud, kui see on rangelt vajalik ning puudutatud isiku õiguste ja vabaduste tagamiseks on võetud asjakohased kaitsemeetmed.

Teabe allikas

- Andmesubjektide liigid: ☒ kõik isikud
- Kujutise allikas: ☒ avalikud kohad
- Seos kuritegevusega: ☒ ei pea tingimata olema otsene geograafiline või ajaline seos
- Teabe kogumise viis: ☒ kaugmeetod

⁹⁰ https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

- Kontekst – mõjutab teisi põhiõigusi: jah, nimelt: ☒ kogunemisvabadus ☒ sõnavabadus ☒ muud õigused
- Võimalikud lisaallikad andmesubjektiga seotud teabe kogumiseks
☒ muu: ei ole välistatud (nt sularahaautomaatide või kaupluste kaamerate kasutamine)

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☒ kuritegevuse valdkonnaga seotud eriandmebaasid

Algoritm

- Töötlemise viis: ☒ üks-mitmele tuvastamine

Tulemus

- Mõju: ☒ otsene (nt andmesubjekt vahistatakse, teda küsitletakse)
- Automatiseeritud töötlusel põhinev otsus: ☒ EI
- Säilitamise kestus: kuni kõigi võimalike uurimiste lõpuni

Õiguslik analüüs

- Andmesubjektile eelnevalt antava teabe liik: ☒ üldteave õiguskaitseasutuse veebilehel
- Kohaldatav õigusraamistik: ☒ valdavalt siseriiklikku õigusesse ülevõetud õiguskaitseidirektiiv ☒ üldine siseriiklik õigus, mis käsitleb biomeetriliste andmete kasutamist õiguskaitseasutuste poolt

5.2. Kohaldatav õigusraamistik

Õiguskaitseidirektiivi artiklit 10 pelgalt kordavad õiguslikud alused ei ole piisavalt selged, et anda üksikisikutele adekvaatset teavet, mis tingimustel ja asjaoludel on õiguskaitseasutustel õigus kasutada avalikes kohtades tehtud videovalveseadmete salvestisi, et luua nende näo biomeetriline mall ja võrrelda seda politseiandmebaasidega. Seega ei vasta käesolevas stsenaariumis mainitud õigusraamistik miinimumnõuetele, et seda saaks kasutada õigusliku alusena⁹¹.

5.3. Vajalikkus ja proportsionaalsus

Vajalikkuse ja proportsionaalsuse lattu nihkub seda kõrgemale, mida rohkem sekkutakse. Avalikes kohtades toimuv biomeetriline kaugtuvastus mõjutab mitmeid põhiõigusi:

Stsenaariumid hõlmavad iga möödakäija jälgimist vastavas avalikus kohas, seega mõjutab see toiming oluliselt elanikkonna mõistlikku ootust jääda avalikes kohtades anonüümseks⁹². See on demokraatliku protsessi paljude aspektide eeltingimus, näiteks soov liituda kodanikuühendusega, võtta osa kogunemistest ning kohtuda mis tahes sotsiaalse ja kultuurilise taustaga inimestega, osaleda poliitilises meeleavalduses ja külastada kõiki võimalikke kohti. Avalikes kohtades anonüümseuse säilitamise kontseptsioon on ülimalt oluline, et teavet ja ideid saaks vabalt koguda ja vahetada. See toetab arvamuste paljusust, rahumeelset kogunemis- ja ühinemisvabadust ning vähemuste kaitset, samuti võimude lahususe ning kontrolli ja tasakaalustatuse põhimõtteid. Avalikes kohtades anonüümseuse säilitamise kontseptsiooni õõnestamine võib avaldada kodanikele tugevalt heidutavat mõju. Nad võivad hoiduda

⁹¹ Kui näotuvastustehnoloogiat kasutamist uuriv teadusprojekt peaks töötleva isikuandmeid, ent selline töötlemine ei kuulu õiguskaitseidirektiivi artikli 4 lõike 3 kohaldamisalasse ega jää väljapoole liidu õiguse kohaldamisala, tuleks kohaldada isikuandmete kaitse üldmäärust. Katseprojektides, millele järgnevad õiguskaitsetoimingud, oleks õiguskaitseidirektiiv kohaldatav.

⁹² EDPB vastus Euroopa Parlamendi liikmetele seoses Clearview AI väljatöötatud näotuvastusrakendusega, 10. juuni 2020, viide: OUT2020-0052.

teatavatest käitumisviisidest, mis on vaba ja avatud ühiskonna osa. See mõjutaks avalikke huve, sest demokraatlik ühiskond nõuab kodanike enesemääramist ja osalemist demokraatlikus protsessis.

Kui sellist tehnoloogiat rakendatakse, piisab lihtsalt vastavas piirkonnas tänavatel, metroos või pagaris käimisest, et õiguskaitseorganid saaksid koguda isikuandmeid, sh biomeetrilisi andmeid, ning esimeses stsenaariumis hõlmaks see ka politsei andmebaasidega võrdlemist. Kui selle asemel rakendatakse sõrmejälgede võtmist, oleks selline olukord selgelt ebaproportsionaalne.

Mõjutatud andmesubjektide arv on äärmiselt suur, sest mõjutatud on kõik, kes mööduvad vastavast avalikust kohast. Lisaks tootsid sellised stsenaariumid kaasa biomeetriliste andmete automatiseeritud massilise töötuse ja ka nende massilise võrdlemise politsei andmebaasidega.

Euroopa kohtupraktikas on massiline jälgimine keelatud (nt Euroopa Inimõiguste Kohus leidis kohtuasjas *S. and Marper vs. Ühendkuningriik*, et biomeetriliste andmete valimatu säilitamine on „ebaproportsionaalne sekkumine“ eraelu puutumatuse õigusesse, sest seda ei peeta „demokraatlikus ühiskonnas vajalikuks“).

Biomeetiline kaugtuvastus on nii lähedane massilisele jälgimisele, et puuduvad usaldusväärsed vahendid piirangute kehtestamiseks. See erineb olemuslikult videoalvest kui sellisest, kuna videosalvestiste võimalik kasutamine ilma biomeetriliste tunnuste tuvastamiseta on juba suur sekkumine, ent ühtlasi piiratud sekkumine, samas kui kohaldatakse näotuvastustehnoloogiat, muudetakse juba laialdaselt kasutatava videoalvesüsteemi kui peamise andmeallika kvaliteeti. Lisaks, eriti mis puudutab sellest tulenevat heidutavat mõju, ei oleks juba olemasolevate videoalveseadmete kohaldamise võimalikud piirangud nähtavad ja seega ei usaldaks avalikkus neid.

Politseiasutuste teostatava biomeetrilise kaugtuvastuse käigus koheldakse igaüht kui potentsiaalset kahtlusallikat. Õigusriigis kehtib aga eeldus, et kodanikud käituvad korrektselt, kuni väärkäitumist on tõendatud. See põhimõte kajastub osaliselt ka õiguskaitsedirektiivis, milles rõhutatakse vajadust teha võimalikult palju vahet kuritegudes süüdi mõistetute ja kahtlusallikate kohtlemisel, sest sellisel juhul peab õiguskaitseasutustel olema „*tõsine alus arvata, et nad on toime pannud või panevad varsti toime süüteo*“ (õiguskaitsedirektiivi artikli 6 punkt a) võrreldes nendega, kes ei ole kuritegudes süüdi mõistetud ega kahtlusallikad.

Transpordisõlmedes või avalikes kohtades rakendatava tehnoloogia abil suudavad õiguskaitseasutused üheselt tuvastada konkreetse isiku ning jälgida ja analüüsida tema liikumist ja asukohti, saades nii teada kõige tundlikumat teavet isiku kohta (isegi tema seksuaalsed sättumused, usulised veendumused, terviseprobleemid). Sellega kaasneb hiiglaslik risk nende andmete ebaseadusliku juurdepääsuks ja kasutamiseks.

Kui me paigaldame süsteemi, mis võimaldab tuvastada inimeste peamised käitumisviisid ja omadused, kaasneb sellega tugev heidutav mõju. Inimesed hakkavad kahtlema, kas nad peaksid teatud meeleväljenduses osalema, mis kahjustaks demokraatlikku protsessi. Kriitiliselt suhtutaks ka sellesse, kui avalikus kohas kohtuda ja veeta aega teatud sõbraga, kellel on teadaolevalt varasemalt probleeme ette tulnud politseiga või kes käitub omapäraselt, sest see ärataks süsteemi algoritmi ja seega ka õiguskaitseasutuste tähelepanu.

Haavatavaid andmesubjekte, näiteks lapsi, ei oleks võimalik kaitsta. Samuti oleks mõjutatud isikud, kellel on professionaalne huvi ja sageli ka vastav juriidiline kohustus hoida oma kontakte konfidentsiaalsena, näiteks ajakirjanikud, advokaadid ja vaimulikud. See võib viia näiteks allika ja ajakirjaniku paljastamiseni või asjaoluni, et isik konsulteerib kriminaalkaitsejaga. Probleem ei puudutaks

ainult juhuslikke avalikke kohti, kus näiteks ajakirjanikud ja nende allikad kohtuvad, vaid ka avalikke kohti, kus saab külastada vastava eriala asutusi või spetsialiste.

Lisaks võib inimeste ebamugavustunne näotuvastustehnoloogia suhtes viia selleni, et nad muudavad oma käitumist, vältivad kohti, kus seda tehnoloogiat kasutatakse, ja tõmbuvad tagasi ühiskondlikust elust ja kultuuriüritustest. Sõltuvalt näotuvastustehnoloogia kasutamise ulatusest võib selle mõju inimestele olla nii märkimisväärne, et mõjutab nende suutlikkust elada väärikat elu⁹³.

Seetõttu esineb suur tõenäosus, et see mõjutab isikuandmete kaitse õiguse olemust, selle puutumatut keset. Ilmsed tunnused (vt suuniste punkt 3.1.3.2) on eelkõige järgmised: õiguskaitseasutused töötlevad suurt hulka inimeste kordumatuid bioloogilisi tunnuseid automaatselt algoritmide abil, mis põhinevad tõenäosusel ja mille tulemused on vaid piiratud määral seletuslikud. Eraelu puutumatuse ja andmekaitse õiguste piirangud kehtestatakse sõltumata isiku individuaalsest käitumisest või temaga seotud asjaoludest. Statistiliselt on peaaegu kõik andmesubjektid, keda sekkumine mõjutab, seaduskuulekad isikud. Andmesubjektile teabe andmise võimalused on piiratud. Kohtusse pöördumine on enamikul juhtudel võimalik alles hiljem.

Tõenäosuslikusel ja piiratud seletuslikkusega süsteemile tuginemine võib põhjustada vastutuse hajutatust ja õiguskaitsevahendite puudumist, ajendades nii seadusrikkumisi.

Kui selline süsteem, mida saab kohandada ka olemasolevate videovalvekaameratega, on kasutusele võetud, võib seda väikese vaevaga ja üksikisikute teadmata kuritarvitada, koostades süstemaatiliselt ja kiiresti inimeste nimekirju etnilise päritolu, soo, usutunnistuse jne alusel. Isikuandmete töötlemist eelnevalt kindlaksmääratud kriteeriumide, näiteks isiku asukoha ja läbitud marsruudi alusel, kasutatakse juba praegu⁹⁴ ja seda võib rakendada diskrimineerivalt.

Vastavalt töödeldavate andmete tundlikkusele, väljenduslikkusele ja hulga suurusele võidakse avalikes kohtades kaugnäotuvastussüsteeme väärkasutada, millel oleks kahjulik mõju puudutatud isikutele. Selliseid andmeid võib samuti kergesti koguda ja väärkasutada, et avaldada survet võimude lahususe ja tasakaalustatuse põhimõttepeamistele tagajatele, nagu näiteks poliitiline opositsioon, ametnikud ja ajakirjanikud.

Näotuvastussüsteemidel kipub olema tugev kallutatus seoses rassi ja sooga: valepositiivsed tulemused mõjutavad ebaproportsionaalselt valgest erineva nahavärviga inimesi ja naisi⁹⁵, põhjustades diskrimineerimist. Valepositiivsele tulemusele järgnevad politseimeetmed, näiteks läbiotsimised ja vahistamised, stigmatiseerivad neid rühmi veelgi.

5.4. Järeldus

Eespool kirjeldatud stsenaariumid, mis käsitlevad biomeetriliste andmete töötlemist läbi kaugmeetodi avalikes kohtades tuvastamise eesmärgil, ei taga õiglast tasakaalu konkureerivate era- ja avalike huvide vahel, moodustades seega ebaproportsionaalse sekkumise harta artiklitest 7 ja 8 tulenevatesse andmesubjektide õigustesse.

⁹³ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, lk 20.

⁹⁴ Vt Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/681 (mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks) artikkel 6 ning Euroopa Parlamendi ja nõukogu 12. septembri 2018. aasta määruse (EL) 2018/1240 (millega luuakse Euroopa reisiinfo ja -lubade süsteem (ETIAS) ning muudetakse määrusi (EL) nr 1077/2011, (EL) nr 515/2014, (EL) 2016/399, (EL) 2016/1624 ja (EL) 2017/2226) artikkel 33.

⁹⁵ <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>,
<http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

6 6. STSENAARIUM

6.1. Kirjeldus

Eraõiguslik üksus pakub rakendust, mille raames näokujutisi kooritakse internetist andmebaasi moodustamiseks.. Kasutaja, näiteks politsei, saab seejärel kujutise üles laadida ja rakendus püüab biomeetrilise tuvastamise abil seda sobitada oma andmebaasis olevate näokujutiste või biomeetriliste mallidega.

Kohalik politseijaoskond uurib parajasti videole jäädvustatud kuritegu, mille puhul ei ole mitmeid võimalikke tunnistajaid ja kahtlusluseid võimalik tuvastada sisemiste andmebaaside või teabega võrdlemise teel. Kogutud teabe põhjal ei ole isikud registreeritud üheski olemasolevas politsei andmebaasis. Politsei otsustab kasutada eespool kirjeldatud vahendit, mida pakub eraettevõtte, et tuvastada isikud biomeetrilise tuvastamise abil.

Teabe allikas

- Andmesubjektide liigid: ☒ kõik kodanikud (tunnistajad) ☒ süüdimõistetud ☒ kahtluslused
- Kujutise allikas: ☒ avalikust kohast või mujalt eeluurimise käigus kogutud videosalvestis
- Seos kuritegevusega: ☒ ei ole vajalik
- Teabe kogumise viis: ☒ kaugmeetod
- Kontekst – mõjutab teisi põhiõigusi: jah, nimelt: ☒ kogunemisvabadus ☒ sõnavabadus ☒ muud õigused: __

Võrdlusandmebaas (millega kogutud teavet võrreldakse)

- Spetsiifilisus: ☒ üldotstarbelised andmebaasid, mis on täidetud internetist saadavate andmetega

Algoritm

- Töötlemise liik: ☒ üks-mitmele tuvastamine

Tulemus

- Mõju ☒ otsene (nt andmesubjekt vahistatakse, teda küsitletakse, teda koheldakse diskrimineerivalt)
- Automatiseeritud töötlusel põhinev otsus: ☒ Ei

Õiguslik analüüs

- Andmesubjektile eelnevalt edastatud teabe liik: ☒ Ei

6.2. Kohaldatav õigusraamistik

Kui eraõiguslik üksus osutab isikuandmete töötlemist hõlmavat teenust, mille eesmärgi ja vahendid on tema määranud (antud juhul nn piltide koorimine internetist, et luua andmebaas), peab sel eraõiguslikul üksusel olema töötlemiseks õiguslik alus. Samuti peab õiguskaitseasutusel, kes otsustab seda teenust enda otstarbeks kasutada, olema töötlemiseks (mille eesmärgid ja vahendid tema kindlaks määrab) õiguslik alus. Et õiguskaitseasutus saaks töödelda biomeetrilisi andmeid, peab olema loodud õiguslik raamistik, milles on sätestatud eesmärk, töödeldavad isikuandmed, töötlemise eesmärgid ja isikuandmete tervikluse ja konfidentsiaalsuse säilitamise ning nende hävitamise kord.

See stsenaarium eeldab massilist isikuandmete kogumist isikutelt, kes ei ole sellest teadlikud. Niisugune töötlemine võib olla seaduslik ainult väga erandlikel asjaoludel. Sõltuvalt sellest, kus

andmebaas asub, võib sellise teenuse kasutamine tähendada isikuandmete ja/või eriliiki isikuandmete edastamist väljapoole Euroopa Liitu (politsei poolt, nt „saadetakse“ jälitusvideost või muul viisil kogutud näokujutis), mistõttu on sellise edastamise jaoks vaja eritingimusi, vt õiguskaitse direktiivi artikkel 39.

Selle stsenaariumi korral ei ole konkreetseid eeskirju, mis lubaksid kirjeldatud töötlemist õiguskaitseasutuse poolt.

6.3. Vajalikkus ja proportsionaalsus

Teenuse kasutamine õiguskaitseasutuse poolt tähendab, et isikuandmeid jagatakse eraõigusliku üksusega, kelle andmebaasi kogutakse isikuandmeid piiramatul ja massilisel viisil. Kogutud isikuandmete ja õiguskaitseasutuse taotletava eesmärgi vahel puudub seos. Andmete edastamine õiguskaitseasutuse poolt eraõiguslikule üksusele tähendab ka seda, et õiguskaitseasutusel puudub kontroll eraõigusliku üksuse töödeldavate andmete üle ning andmesubjektidel on oma õiguste teostamisel suuri raskusi, sest nad ei ole oma andmete sellisest töötlemisest teadlikud. See seab väga ranged tingimused olukordadele, kus selline töötlemine võiks üldse toimuda. On küsitav, kas ükski eesmärk vastaks direktiivis sätestatud nõuetele, sest eraelu puutumatuse ja andmekaitse õiguste erandeid ja piiranguid kohaldatakse ainult juhul, kui see on tingimata vajalik. Üldine huvi võidelda tõhusalt raskete kuritegude vastu ei õigusta iseenesest töötlemist, kui selliseid suuri andmehulki kogutakse andmesubjekte eristamata. Seega ei vastaks selline töötlemine vajalikkuse ja proportsionaalsuse nõuetele.

6.4. Järeldus

Direktiivi artiklite 4 ja 10 nõuetele vastavate selgete, täpsete ja ettenähtavate eeskirjade puudumine ning ka tõendite puudumine, et selline töötlemine on kavandatud eesmärkide saavutamiseks rangelt vajalik, viib järelduseni, et kõnealuse rakenduse kasutamine ei vasta vajalikkuse ja proportsionaalsuse nõuetele ning tähendaks ebaproportsionaalset sekkumist hartast tulenevatesse eraelu puutumatuse ja isikuandmete kaitse õigustesse.