

Sejas atpazīšanas tehnoloģijas un Vispārīgā datu aizsardzības regula



DR. IUR.
IRĒNA NESTEROVA

LU Juridiskās fakultātes Juridiskās
zinātnes institūta pētniece

Mākslīgā intelekta attīstība notiek ļoti strauji. Tas pārveido sabiedrību, veicina efektivitāti gandrīz ikvienā dzīves jomā un sniedz būtiskus ieguvumus daudzās nozarēs, tai skaitā ražošanas, veselības aprūpes un transporta. Mākslīgais intelekts turklāt var palīdzēt risināt globālas sabiedrības problēmas. Tajā pašā laikā mākslīgais intelekts rada arī būtiskus izaicinājumus un riskus sabiedrībai. Mākslīgā intelekta ļaunprātīga vai nolaidīga izmantošana var apdraudēt drošību, pamattiesības un demokrātiju. Lai veicinātu uzticamību un nodrošinātu drošu un taisnīgu mākslīgā intelekta attīstību, Eiropas Savienībā (turpmāk – ES) tiek izstrādātas ētiskās prasības, kā arī pārskatīts tiesiskais regulējums.

Viena no mākslīgā intelekta tehnoloģijām, kas Eiropā ir radījusi plašas diskusijas, ir sejas atpazīšanas tehnoloģijas, kuru izmantošana gan valsts, gan privātajā sektorā strauji pieaug. ES uzticama mākslīgā intelekta izveides ietvaros plāno izstrādāt jaunu regulējumu, lai noteiktu stingras prasības attiecībā uz šo tehnoloģiju izmantošanu. ¹ Šīs tehnoloģijas sāk nonākt arī Eiropas datu aizsardzības iestāžu redzeslokā. Augusta vidū Apvienotās Karalistes datu uzraudzības iestāde uzsāka izmeklēšanu par to izmantošanu *King's Cross* apgabalā Londonas centrā. ² Neilgi pēc tam Zviedrijas datu aizsardzības iestāde piemēroja pirmo sodu par Vispārīgās datu aizsardzības regulas (turpmāk – Regula) ³ pārkāpumu par sejas atpazīšanas tehnoloģiju pret-tiesisku izmantošanu, lai uzraudzītu skolēnu skolas apmeklējumu. ⁴ Ne tikai Eiropā, bet arī citviet pasaulē tiek diskutēts par šo tehnoloģiju izmantošanas robežām. Šī gada maijā Sanfrancisko kā pirmā no ASV pilsētām aizliedza policijas un valsts iestādēm izmantot sejas atpazīšanas tehnoloģijas, kam drīz vien sekoja arī citas ASV pilsētas. ⁵

Rakstā vispirms tiks aplūkoti sejas atpazīšanas tehnoloģiju izmantošanas radītie apdraudējumi, pamatojot nepieciešamību pēc skaidra tiesiskā regulējuma. Mākslīgā intelekta, tai skaitā sejas atpazīšanas tehnoloģiju, regulējuma izstrāde ir jābalsta uz jau spēkā esošajām tiesību normām un prasībām, jo īpaši tām, kas noteiktas Regulā. Raksta turpinājumā tiks aplūkotas tiesību normas, kas noteiktas Regulā, kas jau šobrīd regulē sejas atpazīšanas tehnoloģiju izmantošanu.

Sejas atpazīšanas tehnoloģiju radītais apdraudējums

Līdz ar mākslīgā intelekta sasniegumiem sejas atpazīšanas tehnoloģijas arvien plašāk sāk izmantot gan valsts, gan privātajā sektorā. Sejas atpazīšana ļauj atbloķēt jaunākos viedtālrunus. Dažas bankas, piemēram, Citadele, to izmanto darījumu apstiprināšanai. Sociālais tīkls *Facebook* izmanto sejas atpazīšanu, lai atzīmētu cilvēkus augšupielādētās fotogrāfijās. Lidostas ASV, kā arī Eiropā plāno arvien plašāk izmantot sejas atpazīšanas tehnoloģijas, lai pārbaudītu pasažierus.

Sejas atpazīšanas tehnoloģijas arvien plašāk izmanto arī policijas un citas tiesībaizsardzības iestādes, lai garantētu drošību un cīnītos ar terorismu. Vairākās Eiropas valstīs, piemēram, Apvienotajā Karalistē, Francijā un Vācijā, tiek testētas šīs tehnoloģijas, lai identificētu noziedzniekus un teroristus publiskās vietās, tai skaitā sporta sacensībās un pat Eda Širana mūzikas koncerta laikā. ⁶ Šādi masveida uzraudzības pasākumi netiek regulēti nacionālajos tiesību aktos un ir radījuši plašu sabiedrības satraukumu. Apvienotajā Karalistē, kur ir visplašākā šo tehnoloģiju izmantošana, ir jau ierosinātas pirmās tiesvedības lietas. ⁷

Uzraudzības tehnoloģiju izmantošana būtiski ierobežo cilvēka pamattiesības, jo īpaši tiesības uz privātumu un datu aizsardzību. Līdzās privātuma zaudēšanai pastāv arī risks par mākslīgā intelekta tehnoloģiju neobjektivitāti, kas var novest pie aizspriedumiem un diskriminācijas pret noteiktām grupām vai personām. ⁸ Mākslīgā intelekta sistēmu rezultātus būtiski ietekmē izmantoto datu kvalitāte, kas var atspoguļot neobjektivitāti, neprecizitātes un kļūdas datu vākšanas procesā. Ir veikti pētījumi, kas parāda, ka mākslīgā intelekta algoritmi sejas atpazīšanas tehnoloģijās darbojas atšķirīgi, atkarībā no personas, kura tiek identificēta, vecuma, dzimuma vai etniskās piederības. ⁹ Sejas atpazīšanas tehnoloģijas apstrādā biometriskos datus, kas rada būtiskus un šobrīd pat skaidri nenosakāmus drošības riskus. ¹⁰

Sejas atpazīšanas tehnoloģiju izmantošana rada ne tikai riskus drošībai un pamattiesībām, bet arī grūti paredzamu vai izmērāmu ietekmi, tai skaitā uz demokrātiju un tiesiskumu. Lai gan šīs tehnoloģijas var būt spēcīgs instruments

tiesībaizsardzības iestādēm, lai atrastu aizdomās turētos un teroristus, tās var tikt izmantotas arī cilvēku kontrolei.

Sejas atpazīšanas tehnoloģiju izmantošana masveida uzraudzībai no policijas iestāžu puses tiek salīdzināta ar Ķīnas digitālo uzraudzības sistēmu, kas tiek veidota, izmantojot sejas atpazīšanu un mākslīgo intelektu, kopā ar "sociālā kredīta" sistēmu.¹¹ Šeit arī vietā ir atgādinājums, ka Džordža Orvela pirms 70 gadiem sarakstītais zinātniskās fantastikas romāns "1984" nebija domāts kā instrukcija.¹²

ES 2018. gada aprīlī izveidotā mākslīgā intelekta ekspertu darba grupa vērš uzmanību, ka automatiska identifikācija, tai skaitā sejas atpazīšana un citas piespiedu identifikācijas metodes, kas izmanto biometriskos datus, piemēram, melu atpazīšana, personības vērtēšana ar mikroizpauzsmju palīdzību, automatiska balss atpazīšana, raisa būtiskas juridiskas un ētiskas bažas, jo tai var būt neparedzēta ietekme daudzos psiholoģiskos un sociālkulturālos līmeņos. Tāpat ekspertu grupa vērš uzmanību, ka jebkāda iedzīvotāju vērtēšana var novest pie patstāvības zaudējuma un apdraudēt nediskriminēšanas principu. Vērtēšana būtu jāizmanto tikai tad, ja tā ir skaidri pamatota un ja pasākumi ir samērīgi un taisnīgi. Valsts iestāžu vai privātā sektora personu veikta iedzīvotāju vērtēšana visos aspektos un plašā mērogā apdraud šīs vērtības, jo īpaši, ja to neizmanto saskaņā ar pamattiesībām vai ja to izmanto nesamērīgi, bez skaidri noteikta un paziņota legītīma mērķa. Uzticama mākslīgā intelekta sasniegšanai ir svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automatiski identificētu cilvēkus, un noskaidrot personas identifikāciju no tās izsekošanas, kā arī mērķtiecīgu uzraudzību no masveida novērošanas.¹³

Sejas atpazīšanas tehnoloģiju regulējums

Mākslīgā intelekta, tai skaitā sejas atpazīšanas, tehnoloģijas jau šobrīd regulē spēkā esošās tiesību normas Eiropas, starptautiskajā un nacionālajā līmenī. Mākslīgā intelekta sistēmu izstrādei un izmantošanai ir jāatbilst cilvēktiesību normām, kas noteiktas, piemēram, Eiropas Cilvēka tiesību un pamatbrīvību aizsardzības konvencijā, Eiropas Savienības Pamattiesību hartā un Latvijas Republikas Satversmē. Lai pamattiesību ierobežojumi būtu tiesiski, tiem ir jāatbilst ierobežošanas kritērijiem un ir jābūt stingri nepieciešamiem un samērīgiem.¹⁴ Sejas atpazīšanas tehnoloģijas, jo īpaši masveida uzraudzības pasākumi, var nesamērīgi ierobežot cilvēka pamattiesības, jo īpaši tiesības uz privātumu, pārkāpjot to, kas ir nepieciešams, lai garantētu drošību vai citus legītīmus mērķus.

Mākslīgā intelekta, tai skaitā sejas atpazīšanas tehnoloģiju, izmantošanai ir jāatbilst gan spēkā esošajam tiesiskajam regulējumam, gan uz pamattiesībām balstītajiem ētikas principiem. ES mākslīgā intelekta ekspertu grupa šī gada aprīlī pieņēma Ētikas vadlīnijas uzticamam mākslīgam intelektam (turpmāk – Vadlīnijas), uzsverot, ka mākslīgajam intelektam ir jāatbilst trīs iezīmēm, proti tam ir jābūt: 1) likumīgam – jānodrošina, ka tiek ievēroti visi piemērojamie normatīvie akti; 2) ētiskam – jānodrošina atbilstība ētikas principiem un vērtībām; un 3) noturīgam no tehniskā un sociālā viedokļa, jo mākslīgā intelekta sistēmas var nodarīt netīšu kaitējumu pat tad, ja nodomi ir bijuši labi. Vadlīnijās ir arī formulēti četri ētikas pamatprincipi: 1) cilvēka patstāvības ievērošana, 2) kaitējuma novēršana, 3) taisnīgums un 4) izskaidrojamība. Attīstot šos ētikas principus, Vadlīnijas tālāk nosaka septiņas izpildāmās prasības, kas jāievēro, lai mākslīgais intelekts būtu uzticams: 1) cilvēka subjektivitāte un virsvadība, 2) tehniskā noturība un drošība, 3) privātuma un datu pārvaldība, 4) pārredzamība, 5) daudzveidība, nediskriminēšana un taisnīgums, 6) sabiedrības un vides labklājība, 7) atbildīgums.

Līdzās pamattiesībām un ētikas normām mākslīgā intelekta tehnoloģiju izstrādāšanā un izmantošanā jāņem vērā arī citas prasības, kas noteiktas ES un nacionālajos tiesību aktos, jo īpaši Regulā.

Sejas atpazīšana ietver biometrisku datu apstrādi, kas rada paaugstinātu risku personu tiesībām, un Regula paredz ierobežojumus šādu datu apstrādei. Regula nosaka, ka biometriskie dati ir īpašas kategorijas personas dati, kā arī sniedz biometrisku datu definīciju, proti, tie ir "personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai pirkstu nospiedumi" (4.14. pants).

Biometrisku datu apstrādē ir īpaši būtiski ievērot visus Regulā noteiktos personas datu apstrādes pamatprincipus: likumīgums, godprātība un pārredzamība, nolūka ierobežojumi, datu minimizēšana, precizitāte, glabāšanas ierobežojumi, integritāte un konfidencialitāte, pārskatatbildība (5. pants). Minētie pamatprincipi ir pamatā visām pārējām Regulā noteiktajām prasībām. Eiropas Datu aizsardzības kolēģija (turpmāk – Kolēģija) šī gada jūlijā pieņemtajās Vadlīnijās par personas datu apstrādi, izmantojot videoierīces attiecībā uz biometrisku datu apstrādi, uzsver, ka ir "ārkārtīgi svarīgi, lai šādu tehnoloģiju izmantošana notiktu, pienācīgi ievērojot likumīguma, nepieciešamības, proporcionalitātes un datu minimizēšanas principus".¹⁵

Viens no galvenajiem Regulā noteiktajiem principiem, kas ir jāņem vērā datu pārziņim, izvērtējot sejas atpazīšanas tehnoloģiju izmantošanu, ir nolūka ierobežojuma princips. Tas paredz, ka personas dati tiek vākti konkrētos, skaidros un legītīmos nolūkos un to turpmāka apstrāde netiek veikta ar minētajiem nolūkiem nesavietojamā veidā (Regulas 5.1.b) pants). Kolēģija uzsver, ka, neraugoties uz to, ka šo tehnoloģiju izmantošana var likties īpaši efektīva, pārziņiem vispirms ir jānovērtē to ietekme uz

pamattiesībām un brīvībām un jāapsver mazāk ierobežojoši līdzekļi, lai sasniegtu apstrādes legītīmo mērķi. Zviedrijas datu aizsardzības iestāde augstā pieņēma pirmo lēmumu par Regulas pārkāpumu, kurā konstatēja, ka skolēnu skolas apmeklējuma kontrole nav atzīstams par legītīmu mērķi, kas attaisno sejas atpazīšanas tehnoloģiju izmantošanu.¹⁶

Kolēģija vērš uzmanību, ka "videonovērošana nav uzskatāma par stingri nepieciešamu un samērīgu, ja pastāv citi veidi, kā sasniegt noteikto mērķi. Pretējā gadījumā mēs riskējam ar izmaiņām kultūras normās, kas novestu pie privātuma zuduma jau sākotnējās akceptēšanas".¹⁷ Vēl jo vairāk minētie apsvērumi ir attiecināmi uz videonovērošanu, kas ietver sejas atpazīšanu.

Sejas atpazīšanas tehnoloģiju izmantošanai ir jābūt skaidram pamatojumam. Likumīguma princips paredz, ka personas datu apstrāde var tikt veikta tikai tad, ja tam ir tiesisks pamats. Jāņem vērā, ka īpašu kategoriju personas datu, tai skaitā biometrisko datu, apstrāde ir aizliegta, ja vien nav piemērojams kāds no Regulas 9. panta otrajā daļā noteiktajiem pamatojumiem. Privātajiem uzņēmumiem, lai izmantotu sejas atpazīšanas tehnoloģijas, lielākoties būs jāiegūst personas "nepārprotama piekrišana". ES mākslīgā intelekta ekspertu darba grupa vērš uzmanību, ka, veicot personas automātisku identifikāciju, ar mākslīgā intelekta tehnoloģijām, piemēram, uz priekrišanas pamata, ir jāizstrādā praktiski līdzekļi, kas ļauj sniegt jēgpilnu un pārbaudītu piekrišanu šādi apstrādei.¹⁸

Piekrišanai ir jābūt ne tikai iegūtai atbilstošā veidā, bet ir jāatbilst citiem Regulā noteiktiem kritērijiem, proti, tai ir jābūt brīvai, konkrētai, apzinātai un viennozīmīgai (4.11. pants).¹⁹ Kolēģija uzsver, ka gadījumos, kad piekrišana ir nepieciešama saskaņā ar Regulas 9. pantu, datu pārzinis nedrīkst ierobežot piekļuvi saviem pakalpojumiem atkarībā no piekrišanas sniegšanas biometrisko datu apstrādei. Turklāt, ja autentifikācijai tiek izmantota biometrisko datu apstrāde, datu pārzinim ir jāpieāvā alternatīvs risinājums, kas neietver biometrisko apstrādi bez ierobežojumiem vai papildu izmaksām datu subjektam. Tāpat, paredzot biometriskās ierīces nepieejamību, piemēram, ierīces darbības traucējumu rezultātā, lai nodrošinātu piedāvātā pakalpojuma nepārtrauktību, ir jāievieš rezerves risinājums, kas būtu izmantojams izņēmuma gadījumā.²⁰

Apstrādājot biometriskos datus, ir būtiski ievērot arī citus Regulā noteiktos pamatprincipus un no tiem izrietošās prasības, tai skaitā jāinformē personas par šo tehnoloģiju izmantošanu un jānodrošina citu datu subjekta tiesību īstenošana, jāievieš atbilstoši drošības pasākumi u.c.

Sejas atpazīšanas tehnoloģiju izmantošanas gadījumā pārzinim ir arī jāveic novērtējums par ietekmi uz datu aizsardzību.²¹ Regula nosaka pienākumu veikt novērtējumu, ja apstrādes veids varētu radīt augstu risku fizisku personu tiesībām un brīvībām (35.1. pants). Regula arī paredz, ka novērtējums ir īpaši vajadzīgs, apstrādājot īpašu kategoriju personas datus vai personas datu par sodāmību un pārkāpumiem plašā mērogā (35.3.b) pants), kā arī veicot publiski pieejamu zonu uzraudzību plašā mērogā (35.3.c) pants). Sejas atpazīšanas tehnoloģijas ietver biometrisko datu apstrādi, un to izmantošanas nolūks var būt saistīts ar publiskas telpas uzraudzību plašā mērogā. Datu valsts inspekcijas publicētajā sarakstā ar tām apstrādes darbībām, attiecībā uz kurām ir jāveic novērtējums, ir ietverta "inovatīva jaunu tehnoloģiju vai risinājumu izmantošana vai to pielietošana, piemēram, apvienojot pirkstu nospiedumu un sejas atpazīšanas lietošanu, lai uzlabotu piekļuves kontroli utt."²² Novērtējuma veikšana pirms apstrādes uzsākšanas ļauj novērtēt, vai konkrētajā gadījumā sejas atpazīšanas tehnoloģijas izmantošana ir pieļaujama. Tajā pašā laikā novērtējums atsevišķos gadījumos var nebūt pietiekams, jo līdzās riskiem datu subjekta tiesībām un brīvībām, var būt jāvērtē to plašāka ietekme uz sabiedrību un demokrātiju.

Secinājumi

Līdz ar mākslīgā intelekta sasniegumiem sejas atpazīšanas tehnoloģijas arvien plašāk sāk izmantot gan valsts iestādes drošības nolūkā, gan privātie uzņēmumi, lai veicinātu efektivitāti. Tajā pašā laikā sejas atpazīšanas tehnoloģiju izmantošana būtiski ierobežo pamattiesības, jo īpaši tiesības uz privātumu, un var novest pie diskriminācijas, kā arī rada grūti paredzamu vai izmērāmu ietekmi uz demokrātiju un tiesiskumu. Lai veicinātu uzticēšanos mākslīgā intelekta, tai skaitā sejas atpazīšanas, tehnoloģijām, ir svarīgi skaidri noteikt, vai, kad un kā tās var izmantot.

Mākslīgā intelekta, tai skaitā sejas atpazīšanas tehnoloģiju, izmantošanai ir jāatbilst pamattiesībām, kā arī uz tām balstītajiem ētikas principiem. To izstrādē un izmantošanā ir jāievēro jau šobrīd spēkā esošās tiesību normas un prasības, jo īpaši Regulā noteiktās prasības.

Regula paredz ierobežojumus sejas atpazīšanas tehnoloģiju izmantošanai, ņemot vērā, ka tās ietver biometrisko datu apstrādi, kas rada paaugstinātu risku personu tiesībām. Īpaši būtiski ir ievērot visus Regulā noteiktos personas datu apstrādes pamatprincipus. Viens no pamatprincipiem, kas bija pamatā arī Zviedrijas datu aizsardzības iestādes pirmā soda piemērošanai par sejas atpazīšanas tehnoloģiju prettiesisku izmantošanu, ir nolūka ierobežojuma princips. Tas uzliek pienākumu izvērtēt, vai apstrāde ir nepieciešama un samērīga un vai nepastāv citi mazāk ierobežojoši veidi, kā sasniegt konkrēto nolūku. Tāpat, lai varētu izmantot šīs tehnoloģijas, ir jānodrošina atbilstošs tiesiskais pamats, kas attiecībā uz privāto sektoru lielākoties būs "nepārprotama piekrišana". Datu pārzinis nedrīkst ierobežot piekļuvi saviem pakalpojumiem atkarībā no piekrišanas

sniegšanas biometrisku datu apstrādei. Turklāt, ja šīs tehnoloģijas tiek izmantotas autentifikācijai, ir jāpiedāvā alternatīvs risinājums bez ierobežojumiem vai papildu izmaksām datu subjektam.

Sejas atpazīšanas tehnoloģiju izmantošanas gadījumā jāievēro arī citi Regulā noteiktie pamatprincipi un no tiem izrietošās prasības, tai skaitā jāinformē personas un jānodrošina citu datu subjekta tiesību īstenošana, jāievieš atbilstoši drošības pasākumi un jāveic novērtējums par ietekmi uz datu aizsardzību. Tajā pašā laikā datu aizsardzības prasības var nebūt pietiekamas, jo līdzās riskiem personas tiesībām un brīvībām ir jāvērtē šo tehnoloģiju plašāka ietekme uz sabiedrību un demokrātiju.

Darbs izstrādāts ERAF specifiskā atbalsta mērķa 1.1.1.2. pasākuma "Pēcdoktorantūras pētniecības atbalsts" projekta pētniecības pieteikuma Nr. 1.1.1.2./VIAA/1/16/196 "Taisnīgs līdzsvars starp privātumu un drošību kibertelpā: stingru datu aizsardzības standartu izveide Eiropā" ietvaros.

RAKSTA ATSAUCES / 22

1. Skat.: Khan M. EU plans sweeping regulation of facial recognition. 22.08.2019. Pieejams: <https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9> [aplūkots 28.08.2019.].
2. ICO. Statement: Live facial recognition technology in King's Cross Pieejams: 15.08.2019. Pieejams: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/> [aplūkots 28.08.2019.].
3. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). Pieņemta 04.27.2016. [20.03.2019. red.].
4. EDPB. Facial recognition in school renders Sweden's first GDPR fine. Pieejams: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en [aplūkots 28.08.2019.].
5. Ravani S. Oakland bans use of facial recognition technology, citing bias concerns. 17.07.2019. Pieejams: <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php> [aplūkots 28.08.2019.].
6. Skat.: Burges M. Inside the urgent battle to stop UK police using facial recognition. 17.06.2019. Pieejams: <https://www.wired.co.uk/article/uk-police-facial-recognition> [aplūkots 28.08.2019.].
7. Skat.: Chivers T. Facial recognitionÉ coming to a supermarket near you. Pieejams: <https://www.theguardian.com/technology/2019/aug/04/facial-recognition-supermarket-facewatch-ai-artificial-intelligence-civil-liberties> [aplūkots 28.08.2019.].
8. Skat.: Mākslīgā intelekta augsta līmeņa darba grupa. Etikas vadlīnijas uzticamam mākslīgajam intelektam. 08.04.2019. Pieejamas: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [aplūkotas 28.08.2019.]; EDPB. Guidelines 3/2019 on processing of personal data through video devices. 10.07.2019. Pieejams https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [aplūkots 28.08.2019.]; Wall M. Biased and wrong? Facial recognition tech in the dock, 08.07.2019. Pieejams: <https://www.bbc.com/news/business-48842750> [aplūkots 28.08.2019.].
9. Skat.: EDPB. Guidelines 3/2019 on processing of personal data through video devices. 10.07.2019. Pieejams https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [aplūkots 28.08.2019.]; Wong Q. Why facial recognition's racial bias problem is so hard to track. 27.03.2019. Pieejams: <https://www.cnet.com/news/why-facial-recognitions-racial-bias-problem-is-so-hard-to-crack/> [aplūkots 28.08.2019.].
10. Skat.: Doffman Z. New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report. 14.08.2019. Pieejams: <https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#76f9901046c6> [aplūkots 28.08.2019.].
11. Skat.: Corney M. Leave no dark corner. 17.08.2018. Pieejams: http://mobile.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278?pfmredir=sm&sf197878142=1&smid=Page:%20ABC%20Australia-Facebook_Organic&WT.src=Facebook_Organic [aplūkots 28.08.2019.].
12. Skat.: Esteve F. Orwell in times of facial recognition. 18.08.2018. Pieejams: <http://lab.cccb.org/en/orwell-in-times-of-facial-recognition/> [aplūkots 28.08.2019.].
13. Mākslīgā intelekta augsta līmeņa darba grupa. Etikas vadlīnijas uzticamam mākslīgajam intelektam. 04.2019. Pieejamas: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [aplūkotas 28.08.2019.].
14. Eiropas Savienības Pamattiesību hartas 52. panta pirmā daļa paredz, ka tiesību un brīvību izmantošanas ierobežojumiem ir: jābūt noteiktiem tiesību aktos; jārespektē tiesību un brīvību būtība; jāatbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības; jābūt nepieciešamiem; jābūt samērīgiem.
15. EDPB. Guidelines 3/2019 on processing of personal data through video devices. 10.07.2019. Pieejams: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [aplūkots 28.08.2019.].
16. Skat.: Facial recognition: School ID checks lead to GDPR fine. 27.08.2019. Pieejams: https://www.bbc.com/news/technology-49489154?ocid=socialflow_twitter [aplūkots 28.08.2019.].

17. EDPB. Guidelines 3/2019 on processing of personal data through video devices. 10.07.2019. Pieejams: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [aplūkots 28.08.2019.]
18. Mākslīgā intelekta augsta līmeņa darba grupa. Etikas vadlīnijas uzticamam mākslīgajam intelektam. 04.2019. Pieejamas: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> [aplūkotas 28.08.2019.].
19. Plašāk skat.: Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679. 28.11.2017. Pieejams: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [aplūkots 28.08.2019.].
20. EDPB. Guidelines 3/2019 on processing of personal data through video devices. 10.07.2019. Pieejams: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf [aplūkots 28.08.2019.].
21. Turpat.
22. Datu valsts inspekcija. Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu. Pieejams: <https://www.dvi.gov.lv/lv/wp-content/uploads/Saraksts-ar-tiem-apstrades-darbibas-veidiem-attieciba-uz-kuriem-ir-javeic-novertejums-par-ietekmi-uz-datu-aizsardzibu-NIDA1.pdf> [aplūkots 28.08.2019.].

ATSAUCE UZ ŽURNĀLU

Ņesterova I. Sejas atpazīšanas tehnoloģijas un Vispārīgā datu aizsardzības regula. Jurista Vārds, 24.09.2019., Nr. 38 (1096), 27.-31.lpp.