ierobežojuši 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 biometrisko 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. ■

Foto: Boriss Kolesņikovs

NUMURA TĒMA:
KO GAIDĪT
NO MĀKSLĪGĀ
INTELEKTA

Mg. iur., MA grāds informācijas tehnoloģiju tiesībās
Jūlija Terjuhana
ZAB "Sorainen" juriste, sertificēta datu aizsardzības speciāliste

Mākslīgā intelekta trenēšana, izmantojot personas datus

Ievads

Mākslīgais intelekts ir datorzinātnes apakšnozare, kas nodarbojas ar intelektuālas uzvedības automatizāciju. Mākslīgo intelektu definē arī kā pētījumus, kā likt datoriem darīt lietas, ko pašlaik cilvēki dara labāk, vai kā skaitļošanas procesu pētījumus, kas ļauj uztvert, spriest un darboties.[1]

Agrīnā mākslīgā intelekta pētījumi aizsākušies 20. gs. četrdesmitajos gados. Pirmais pašlaik plaši pazīstamais mākslīgā intelekta darbs ir Vorena Makaloha (*Warren McCulloch*) un Voltera Pitsa (*Walter Pitts)* 1943. gadā izstrādātais mākslīgā neirona modelis. Terminu "mākslīgais intelekts" 1956. gadā ieviesis Džons Makārtijs (*John McCarthy*). Kopš 20. gs. piecdesmitajiem gadiem, piedzīvojot kāpumus un kritumus,[2] ir turpinājusies mākslīgā intelekta attīstība.

20. gs. astoņdesmitajos gados mākslīgā intelekta tēma ieguva rezonansi pasaules kinoindustrijā, radot skatītājiem paliekošu iespaidu, ka cilvēku pasauli reiz savā varētu pārņemt saprātīgas mašīnas, taču šis priekšstats neatspoguļo visu mākslīgā intelekta spektru un ir radījis paliekošus mītus sabiedrībā, kas to aizvien satrauc.

Literatūrā[3] ir aprakstīti dažādi veidi, kā iespējams klasificēt mākslīgo intelektu. Uz to var lūkoties caur mākslīgā intelekta evolūcijas prizmu, kas klasificē mākslīgo intelektu pēc tā attīstības stadijām – mākslīgais šaurais intelekts (*artificial narrow intelligence*), mākslīgais vispārīgais intelekts (*artificial general intelligence*) un mākslīgais superintelekts (*artificial super intelligence*).[4] Ar šauro mākslīgo intelektu jāsaprot tāds mākslīgais intelekts, kas pārsniedz cilvēka spējas kādā šauri nodefinētā jomā. Savukārt mākslīgais vispārīgais intelekts un superintelekts

1 Grundspeņķis J. Mākslīgais intelekts. Grām.: Nacionālā enciklopēdija. Pieejams: *https://enciklopedija.lv/skirklis/24447-mākslīgais-intelekts* [aplūkots 03.09.2019.].

2 Laika periodus 1974.–1980. un 1987.–1993. gads ir pieņemts uzskatīt par t.s. mākslīgā intelekta ziemu, kad šī joma piedzīvoja finansējuma, pētnieku uzmanības un attīstības kritumu. Boobier T. Advanced Analytics and AI: Impact, Implementation, and the Future of Work. John Wiley & Sons, 2018, p. 41.

3 Marr D. Artificial intelligence – A personal view. Artificial Intelligence. Vol. 9, Issue 1, 1977, pp. 37–48; Yunhe P. Heading toward Artificial Intelligence 2.0. Engineering, Vol. 2, Issue 4, 2016, pp. 409–413.

4 Kaplan A., Haenlein M. Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. Business Horizons, 2019, 62 (1). Pieejams: *https://www.sciencedirect.com/science/article/pii/S0007681318301393#* [skatīts 03.09.2019.].

vēl ir nākotnes tehnoloģijas, kas var tikt vai netikt radītas. Vispārīgais mākslīgais intelekts būs sasniegts tad, kad tehnoloģijas pilnībā varēs darboties ar cilvēka kognitīvo[5] spēju kapacitāti, savukārt superintelekts – kad tehnoloģiju kognitīvās spējas būtiski pārspēs cilvēka kognitīvās spējas uzdevumu izpildē, analizē, lēmumu pieņemšanā un tam piemitīs sevis apzināšanās spēja.[6]

Mākslīgo intelektu var iedalīt trīs dažādās kompetenču sistēmās: analītiskajā, cilvēka iedvesmotā un humanizētā mākslīgajā intelektā. Analītiskais mākslīgais intelekts rada kognitīvu pasaules attēlojumu un izmanto pagātnes pieredzē balstītas mācības, lai informētu par turpmākiem lēmumiem. Cilvēka iedvesmotā mākslīgajā intelektā ir elementi no kognitīvās un emocionālās inteliģences – cilvēka emociju izpratne papildus kognitīvajiem elementiem un to apsvēršana lēmumu pieņemšanā. Humanizētais mākslīgais intelekts parāda visu veidu kompetenču īpašības (t.i., kognitīvā, emocionālā un sociālā inteliģence), un tas spēj būt pašapzinīgs un apzināti mijiedarboties.[7]

Šobrīd tehnoloģijas ir attīstījušās šaurā mākslīgā intelekta līmenī, tas ir analītiskais mākslīgais intelekts, kas pieņem lēmumus kādā šauri definētā jomā. Tikmēr zinātnieki un praktiķi turpina darbu pie attīstītāku mākslīgā intelekta modeļu izstrādes.

Mākslīgais intelekts tiek izmantots mūsdienās daudzās nozarēs, piemēram, banku un finanšu, medicīnā, e-komercijā, militārajā jomā, aviācijā, lingvistikā, mūzikas industrijā, transporta industrijā u.c. Mākslīgo intelektu arvien biežāk izmanto ne tikai komersanti, bet arī valsts institūcijas, lai automatizētu klientu apkalpošanu, atvieglotu iedzīvotājiem saziņu ar valsti, analizētu klientu apmierinātību, veiktu nākotnes prognozes u.c.[8] Mākslīgais intelekts tiek plaši izmantots, lai veiktu digitālā satura analīzi un radītu saturu, prognozētu rīcības modeļus, automatizētu lēmumu pieņemšanu, to izmanto viedierīcēs, viedo asistentu tehnoloģijās un citur. Mākslīgais intelekts palīdz analizēt jau esošos datus un rīcības un, veicot datu analīzi, mācās nonākt pie jauniem risinājumiem.

Mākslīgā intelekta tehnoloģijām nonākot saskarsmē ar gala lietotāju, arī tiesību zinātne ir spiesta šķērsot robežu starp tiesību zinātni un datorzinātni, lai izprastu tehnoloģiju sniegtās iespējas, iespējamos riskus un to ietekmi uz indivīdu tiesību īstenošanu.

Personas attēlos balstīta mākslīgā intelekta trenēšana

Mākslīgā intelekta apmācīšanai jeb trenēšanai tiek izmantota jau esošo datu analīze. Atkarībā no tā, kāds ir mākslīgā intelekta programmas uzdevums, var būt situācijas, kad mākslīgā intelekta tehnoloģijas veic tādu datu analīzi, kas ir uzskatāmi par personas datiem, t.i., datiem, kas attiecas uz identificētu vai identificējamu fizisku personu. Šādos gadījumos ir būtiski ņemt vērā ne tikai mākslīgā intelekta izstrādātāja intereses izstrādāt jaunu produktu vai uzlabot esošo pakalpojumu kvalitāti, bet arī to personu intereses uz savu datu un privātuma aizsardzību, kuru dati tiek izmantoti mākslīgā intelekta apmācībā.

Viens no personas datu veidiem ir personas attēls, kas šobrīd arvien biežāk tiek izmantots, lai radītu lietotājam pievilcīgu produktu. Piemēram, sejas attēla analīze tiek izmantota autentifikācijas nolūkos viedierīcēs un izklaides nolūkos populārajās mobilajās aplikācijās,[9] kurās lietotājam viedierīces kamerā ir redzami dažādi sejas attēla filtri. Taču tā tiek izmantota arī tehnoloģijās, kas palīdz valsts iestādēm izmeklēt noziedzīgus nodarījumus un nodrošināt sabiedrisko kārtību tādās valstīs kā Lielbritānija,[10] ASV, Ķīna un citur. Tādējādi mākslīgā intelekta lēmumi skar gan indivīdu privāto dzīvi, gan attiecības ar valsti.

> Mākslīgo intelektu var iedalīt trīs dažādās kompetenču sistēmās: analītiskā, cilvēka iedvesmotā un humanizētā mākslīgajā intelektā.

Lai trenētu mākslīgo intelektu, arvien biežāk fotoattēli tiek izmantoti no brīvpiekļuves interneta resursiem, iegūstot tūkstošiem attēlu bez tajos redzamo cilvēku ziņas, klasificējot attēlus pēc vecuma, dzimuma, ādas toņa un desmitiem citu rādītāju. "Tas ir mākslīgā intelekta trenēšanas mazais, netīrais noslēpums," atzīst Ņujorkas Universitātes Juridiskās fakultātes profesors Džeisons Šulcs (*Jason M. Schultz*).[11]

Šī raksta mērķis ir izcelt problemātiskos aspektus, kad internetā brīvi pieejamu fotogrāfiju izmantošana mākslīgā intelekta trenēšanai var radīt privātuma aizskārumu, vērst uzmanību uz aspektiem, kas jāņem vērā, ja izstrādātāji vēlas īstenot šo procesu tiesiski un respektējot

5 Kognitīvs – ar izziņu (izzinātājdarbību) saistīts; tāds, ka pamatā ir izziņa (izzinātājdarbība). Svešvārdu vārdnīca. Rīga: Jumava, 2007.

6 Bostrom N. Superintelligence: Paths, Dangers, Strategies. Oxford University Press, 2014.

7 Kaplan A., Haenlein M. Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. Business Horizons, 2019, 62 (1). Pieejams: *https://www.sciencedirect.com/science/article/pii/S0007681318301393#* [skatīts 03.09.2019.].

8 Ratkevičs J. Mākslīgais intelekts un tā izmantošana valsts sektorā. Pieejams: *https://www.lps.lv/uploads/docs_module/1_1_M%C4%81ksl%C4%ABgais%20intelekts%20un%20t%C4%81%20izmanto%C5%A1ana%20valsts%20sektor%C4%81.pdf*

9 Le J. Snapchat's Filters: How computer vision recognizes your face. The science behind personalized facial recognition. 29.01.2018. Pieejams: *https://medium.com/cracking-the-data-science-interview/snapchats-filters-how-computer-vision-recognizes-your-face-9907d6904b91* [skatīts 12.09.2019.].

10 Murgia M. How London became a test case for using facial recognition in democracies. Fanancial Times, 01.08.2019. Pieejams: *https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959* [skatīts 14.09.2019.].

11 Solon O., Farivar C. Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools. 12.03.2019. Pieejams: *https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921* [skatīts 14.09.2019.].

personu privātumu, kā arī ieskicēt Eiropas Savienības (turpmāk – ES) regulējuma tendences turpmākai mākslīgā intelekta attīstībai.

Datu apstrādes tiesiskais pamats, datu apstrādes principi un datu subjekta informēšana

No juridiskā viedokļa raugoties, personas sejas attēls ir uzskatāms par personas datiem, bet tajā attēlotā persona – par datu subjektu. Datu aizsardzības prasības ES un Eiropas Ekonomiskajā zonā regulē Vispārīgā datu aizsardzības regula[12] (turpmāk – VDAR), kas ir tieši piemērojama visās dalībvalstīs, kā arī to papildina nacionālie normatīvie akti. Uz komersantiem, kas veic viņu datu apstrādi ES/EEZ teritorijā, attiecas VDAR noteikumi gadījumos, ja komersants ir reģistrēts ES/EEZ vai informācijas sabiedrības pakalpojums ir adresēts gala lietotājiem ES/EEZ, vai arī veic datu subjektu uzvedības novērošanu ES/EEZ. VDAR ikvienam datu pārzinim, kurš nosaka sevis izvēlētus mērķus un līdzekļus personas datu apstrādei, uzliekt par pienākumu ievērot VDAR prasības un principus, tostarp informēšanas pienākumu par pašu datu apstrādes faktu.

Fotoattēlos redzamās personas, kas (kaut arī brīvprātīgi) var būt publicējušas savu attēlu kādā no mājaslapām, piemēram, sociālajos tīklos, aizvien bauda tiesības uz savu datu aizsardzību. Šādās vietnēs personas datu pārzinis ir komersants, kurš sniedz pakalpojumu.

VDAR 6. pants nosaka, ka jebkurai datu apstrādei ir jābūt balstītai uz tiesisku pamatu. Pamats var būt piekrišana, iestāšanās līgumattiecībās vai līguma izpilde, normatīvo aktu prasības, datu subjekta vitālo interešu aizsardzība, sabiedrības intereses vai pārziņa leģitīmās intereses. Tiesiskais pamats attiecībām starp interneta platformām un to lietotāju ir pakalpojuma līgums, kura noteikumiem lietotājs piekrīt, reģistrējoties portālā. Savukārt komersants uzņemas apstrādāt datus saskaņā ar privātuma politiku un vietnes saistošajiem noteikumiem vai ar lietotāju noslēgto līgumu. Noteikumiem vai līgumam ir jāatbilst VDAR prasībām.

Neatkarīgi no tā, kurš no minētajiem pamatiem ir datu apstrādes pamatā, VDAR 13. un 14. pants nosaka pārziņa pienākumu informēt datu subjektu par datu apstrādi un datu subjekta tiesībām gan gadījumos, kad tas ievāc datus pa tiešo no datu subjekta, gan tad, ja tas saņem datus no kāda cita komersanta vai iestādes. Papildus tam vienmēr, veicot datu apstrādi, pārzinim ir jāievēro VDAR 5. pantā noteiktie datu apstrādes principi, kā arī princips "privātums pēc noklusējuma un integrēta datu aizsardzība", kas nozīmē, ka ikvienai tehnoloģijai, kas tiek radīta, ir jāfunkcionē tā, lai tā respektētu personu privātumu.

Tādējādi nebūtu pieļaujams, ka ikviens uzņēmums varētu brīvi iegūt un izmantot savām vajadzībām jebkādus interneta vietnēs pieejamus personas datus, tostarp fotogrāfijas, bez datu subjektu informēšanas un bez tiesiska pamata šādu datu apstrādei.

Tālāk paraudzīsimies uz diviem publiski izskanējušiem gadījumiem, kad mākslīgā intelekta trenēšanai ir izmantotas interneta platformās atrodamās lietotāju fotogrāfijas.

International Business Machines Corporation (IBM) piemērs[13]

2019. gada martā ASV medijs *NBC News* publicēja informāciju par to, ka viens no vadošajiem tehnoloģiju uzņēmumiem IBM veic savu mākslīgā intelekta programmu trenēšanu, izmantojot publiski pieejamās populārās fotogrāfiju uzglabāšanas platformas *Flickr* lietotāju fotogrāfijas.

Kļuva zināms, ka IBM izmantoja sava mākslīgā intelekta trenēšanai tos attēlus, kas ir publiski pieejami *Flickr* ar t.s. *Creative Commons* nekomerciālo licenci. Attēlus ir augšupielādējuši platformas lietotāji, ļaujot, lai citi lietotāji tos varētu izmantot savos komerciālos mērķos. Lai gan šajā gadījumā IBM nepublicēja šīs fotogrāfijas komerciāliem mērķiem, ir jāņem vērā, ka fotogrāfija ir komplekss objekts, kas aptver vairāku juridisku jautājumu kopumu. *Creative Commons* autortiesību licence pati par sevi skar autortiesību noregulējumu, bet nekādi neatrunā attēlos redzamo personu tiesības, neizslēdz lietotāju, kas augšupielādējis attēlus, informēšanu par to, ka viņu augšupielādētie dati tiks izmantoti, un nesniedz komersantam personas atļauju rīkoties ar saviem datiem.

Flickr gadījumā desmitiem tūkstošu lietotāju dati tika izmantoti mākslīgā intelekta trenēšanai, faktiski – izmantoti jauna produkta izstrādei, ko veic cits, ar *Flickr* nesaistīts komersants. *Flickr* lietotājiem netika sniegta informācija par viņu datu izmantošanu. Tāpat nepastāvēja neviens no VDAR paredzētajiem tiesiskajiem pamatiem datu apstrādei – IBM nebija līguma attiecību ar *Flickr* lietotājiem, netika saņemta arī lietotāju piekrišana, kā arī nepastāvēja neviens no pārējiem iespējamiem datu apstrādes pamatiem.

Facebook piemērs[14]

2018. gada maijā izskanēja ziņas, kas *Facebook* īpašumā esošās mobilās lietotnes *Instagram* veidotāji izmantoja aptuveni 3,5 miljardus lietotnes lietotāju fotoattēlus ar mērķi trenēt mākslīgo intelektu. Ar automatizētiem līdzekļiem

12 Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) 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) 4. pants. OV L 119, 04.05.2016., 1.–88. lpp.

13 Solon O., Farivar C. Millions of people uploaded photos to the Ever app. Then the company used them to develop facial recognition tools. 12.03.2019. Pieejams: *https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921* [skatīts 14.09.2019.].

14 Shead S. Facebook Used 3.5 Billion Public Instagram Photos To Train AI. 03.05.2018. Pieejams: *https://www.forbes.com/sites/samshead/2018/05/03/facebook-used-3-5-billion-public-instagram-photos-to-train-ai/#786cf896d4ad* [skatīts 14.09.2019.].

tika apstrādāti attēli, pie kuriem ir norādīta kāda konkrēta mirkļbirka jeb tēmturis (*hashtag*). Mirkļbirkas lietošana ļauj *Instagram* rīcībā esošos datus sadalīt pa kategorijām, kuras attēliem piešķīruši lietotāji. Mirkļbirkas visbiežāk atspoguļo attēlā redzamo priekšmetu, personu (piemēram, *#motheroftwins, #lawyer*) notikumu vai kontekstu (piem., *#vacation, #food, #backtoschool* u.tml.). Programma tādā veidā apguva prasmi, kas parasti ietilpst cilvēka uzdevumā – atpazīt attēlā redzamo objektu. Autori norāda, ka *Facebook* izmantotais datu apjoms ir desmitreiz lielāks nekā līdz šim kompānijas *Google* izmantotais fotoattēlu kopums, ko tā izmantoja mākslīgā intelekta trenēšanai.

Lai trenētu mākslīgo intelektu, arvien biežāk fotoattēli tiek izmantoti no brīvpiekļuves interneta resursiem, iegūstot tūkstošiem attēlu bez tajos redzamo cilvēku ziņas, klasificējot attēlus pēc vecuma, dzimuma, ādas toņa un desmitiem citu rādītāju.

Vai arī šajā gadījumā noticis datu subjektu tiesību aizskārums, un vai *Facebook* ir rīkojies negodprātīgi? Lai to noskaidrotu, ir vērts rūpīgāk ielūkoties lietotnes *Instagram* lietošanas noteikumos,[15] kas atšķirībā no IBM gadījuma kalpo par datu tiesisko pamatu starp uzņēmumu un lietotāju vietnes privātuma politikā.[16]

Instagram lietošanas noteikumi satur skaidru norādi uz mākslīgā intelekta un mašīnmācīšanās izmantošanu *Instagram* pakalpojumu uzlabošanai, savukārt *Instagram* privātuma politika satur informāciju par to, ka *Instagram* māteskompānija *Facebook* izmanto sejas atpazīšanas tehnoloģiju, kā arī satur hipersaiti uz attiecīgajiem noteikumiem. *Facebook* izmanto *Instagram* lietotāju datus, izmantojot sejas atpazīšanas metodi, ja vien lietotājs savā profilā nav atspējojis šo opciju. Savukārt *Instagram* pakalpojums pats par sevi sejas atpazīšanas tehnoloģiju (vēl) neizmanto.

Tādējādi *Facebook* un *Instagram* lietotājam tiek sniegta informācija VDAR 13. un 14. panta izpratnē, tam ir iespēja iepazīties ar lietotņu privātuma un lietošanas noteikumiem, veikt izmaiņas uzstādījumos, kā arī īstenot savas VDAR noteiktās datu subjekta tiesības, vēršoties pie šiem uzņēmumiem.

Lai gan risinājums, kā tiek nodrošināta piekļuve informācijai par datu apstrādi un sejas atpazīšanas atspējošanu, varētu tikt kritizēts, šajā gadījumā pastāv tiesiskais pamats datu apstrādei un tiek nodrošināta lietotāja informēšana par viņa datu apstrādi. Informētībai par datu pārzini un savām tiesībām ir būtiska loma datu subjekta tiesību aizsardzībā gadījumos, kad viņam rodas šaubas par datu apstrādes tiesiskumu vai viņa tiesības ir aizskartas.

Mākslīgais intelekts un personas dati – ES pieeja

Mākslīgā intelekta regulējuma jautājums pēdējos gados ir ieņēmis redzamu lomu ES. Viens no lielākajiem mākslīgā intelekta izaicinājumiem ir rast balansu starp tehnoloģiju attīstību un indivīda tiesībām šīs tehnoloģijas izmantošanā.

2018. gadā Eiropas Komisija izveidoja augsta līmeņa neatkarīgo ekspertu grupu, lai izstrādātu ētikas vadlīnijas mākslīgā intelekta izstrādē un iedzīvinātu tās praksē,[17] kā arī izstrādāja mākslīgā intelekta stratēģiju, novietojot tehnoloģisko iespēju attīstības centrā cilvēku, t.i., viņa vajadzības un tiesības. 2018. gada jūnijā Komisija publicēja Uzticama mākslīgā intelekta vadlīnijas. Vadlīnijas uzsver tādu vērtību kā ētiskums, taisnīgums un nediskriminācija, pārredzamība, cilvēka virsvadība, drošums, atbildība, privātums un datu aizsardzības ievērošanas pienākums, izstrādājot mākslīgā intelekta tehnoloģijas.

Savukārt 2019. gada janvārī Eiropas Padomes Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi[18] konsultatīvā komiteja publicēja Vadlīnijas par mākslīgo intelektu un datu apstrādi[19] (*Guidelines on Artificial Intelligence and Data Protection*), lai palīdzētu mākslīgā intelekta izstrādātājiem, ražotājiem, pakalpojumu sniedzējiem, kā arī likumdevējiem nodrošināt tādu mākslīgā intelekta attīstību un tehnoloģiju izmantošanu, kas respektētu personas tiesības uz datu aizsardzību. Šīs vadlīnijas atgādina par to, ka saskaņā ar VDAR nostiprinātajām prasībām jāievēro datu apstrādes principi un Konvencijas pamatvērtības un jārespektē datu subjekta tiesības, kā arī uzsver indivīda kontroles nozīmīgumu pār saviem personas datiem, tostarp, ja mākslīgais intelekts tiek izmantots automatizētu lēmumu pieņemšanā.

Lai gan vadlīnijām nepiemīt normatīvā akta spēks un ES nereti tiek adresēts atgādinājums, ka informācijas tehnoloģiju progress nebūtu iespējams pārregulētā vidē, tomēr ir būtiski ņemt vērā, ka arī interneta vidē nevalda visatļautība. Vadlīnijas vēlreiz uzsver, ka tiesības, kas nostiprinātas Konvencijā un indivīdiem piemīt dzīvē, piemīt tiem arī digitālajā vidē. ■

15 Instagram Terms of Use. Pieejams: *https://help.instagram.com/581066165581870*

16 Instagram Data Policy. Pieejams: *https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center*

17 Mākslīgais intelekts: Komisija turpina darbu ar ētikas vadlīnijām. 08.04.2019. Pieejams: *https://ec.europa.eu/digital-single-market/en/artificial-intelligence* [skatīts 14.09.2019.].

18 Eiropas Padomes Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi Eiropas Padome, 28.01.1981. Latvijas Republikas Saeima apstiprinājusi šo konvenciju 2001. gada 5. aprīlī ar likumu "Par Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi".

19 Consultative Committee of The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (Convention 108) Guidelines on Artificial Intelligence and Data Protection. Adopted on 25.01.2019. Pieejams: *https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8* [skatīts14.09.2019.].