Pētījums mākslīgā intelekta sistēmas un diskriminācijas aspekti

Autore: Dr.iur. Irēna Barkāne

2024

LATVIJAS REPUBLIKAS TIESĪBSARGS

LATVIJAS UNIVERSITĀTE

Saturs

Vāka attēlu Tiesībsarga birojs izveidoja ar ChatGPT, izmantojot DALL-E attēlu veidošanas rīku.

Saīsinājumi

Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija - ECTK

Eiropas Savienība – ES

ES Pamattiesību harta – Harta

Mākslīgais intelekts – MI

Mākslīgā intelekta akts – MI akts

Vispārīgajai datu aizsardzības regula – VDAR

1. Ievads

Eiropas Savienībā (ES) 2024. gada 13. jūnijā tika pieņemta Eiropas Parlamenta un Padomes Regula 2024/1689, kas nosaka saskaņotas normas mākslīgā intelekta jomā – Mākslīgā intelekta akts (MI akts).[1] MI akts tika publicēts ES Oficiālajā Vēstnesī 2024. gada 12. jūlijā un stājās spēkā 1. augustā. Tas kļūs tieši piemērojams visās ES dalībvalstīs, tai skaitā Latvijā, pēc diviem gadiem, t.i. no 2026. gada 2. augusta, izņemot atsevišķus noteikumus, kas tiks piemēroti ātrāk.

MI aktā ir izmantota uz risku balstīta pieeja, klasificējot MI sistēmas atkarībā no dažādiem to radītajiem riska līmeņiem. Mākslīgā intelekta (MI) sistēmas, kas tiek klasificētas kā augsta riska sistēmas, var radīt kaitējumu plašam pamattiesību klāstam. MI aktā ir norādīts, ka tam, cik liela ir MI sistēmas izraisītā kaitējošā ietekme uz ES Pamattiesību hartā[2] (Harta) aizsargātajām pamattiesībām, ir īpaši svarīgi, klasificējot MI sistēmu kā augsta riska. Minētās tiesības ietver tiesības uz cilvēka cieņu, privātās un ģimenes dzīves neaizskaramību, personas datu aizsardzību, vārda un informācijas brīvību, pulcēšanās un biedrošanās brīvību, tiesības uz izglītību, patērētāju tiesību aizsardzību, darba ņēmēju tiesības, personu ar invaliditāti tiesības, dzimumu līdztiesību, intelektuālā īpašuma tiesības, tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, tiesības uz aizstāvību un nevainīguma prezumpciju, tiesības uz labu pārvaldību, kā arī diskriminācijas aizliegumu (MI akta 48. apsvērums). Diskriminācijas aizliegums ir vienas pamattiesībām, kas tiek visbiežāk pārkāptas MI sistēmu izmantošanas rezultātā, kā to parādīs Pētījumā aplūkotie prakses piemēri.

Pētījuma mērķis ir izpētīt MI sistēmu jau šobrīd radītos diskriminācijas riskus četrās no MI akta II pielikumā minētajām jomām:

1) fizisku personu biometriskā identifikācija un kategorizācija;

2) izglītība un arodapmācības;

3) nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai;

[1] Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/.

[2] Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. *OV C* 2020/239, 07.06.2016.

4) piekļuve privātiem pamatpakalpojumiem un sabiedriskajiem pakalpojumiem un pabalstiem un to izmantošana.

Tajā pašā laikā ir jānorāda, ka MI sistēmas var radīt diskriminācijas riskus arī daudzās citās jomās, piemēram, migrācijas un patvēruma jomā, veselības aprūpes jomā, veicināt vardarbību dzimuma dēļ un naida runu digitālajā vidē, it īpaši sociālo mediju platformās. Tomēr šīs jomas ir ārpus šajā pētījumā apskatāmo jautājumu loka.

Pētījuma sākumā ir analizēts diskriminācijas aizlieguma, datu aizsardzības un mākslīgā intelekta normatīvais regulējums, kā arī vērsta uzmanību uz esošā tiesiskā regulējuma problēmām un izaicinājumiem algoritmu un MI sistēmu izmantošanas kontekstā. Pēc tam Pētījumā ir apkopoti un analizēti uzskatāmākie piemēri no starptautiskās prakses, kas saistīti ar MI sistēmu radīto diskrimināciju iepriekš minētajās četrās jomās.

Pētījumā pamatā tiek analizēti piemēri no prakses par MI sistēmu radīto diskrimināciju šādu kritēriju dēļ – dzimums, invaliditāte, rase, etniskā piederība, sociālais stāvoklis, vecums, seksuālā orientācija. Tajā pašā laikā pētījumā tiek apskatīti arī piemēri par to, kā MI sistēmu izmantošana citu kritēriju dēļ var radīt pozitīvu/negatīvu attieksmi iepriekš minētajās jomās.

Pētījuma nobeigumā tiks sniegts kopsavilkums, kurā apkopota būtiskākā informācija par Pētījuma rezultātiem, secinājumi un ieteikumi.

Pētījumā ir izmantoti Latvijas, Eiropas vai citu valstu autoru pētījumi par MI sistēmu un algoritmisko diskrimināciju. Pētījumā ir apkopots un analizēts ES, kā arī Latvijas tiesiskais regulējums un starptautiskā prakse. Latvijā cilvēktiesību aizsardzības iestāde, Latvijas Republikas Tiesībsarga birojs, līdz šim nav izskatījis lietas, kas saistītas ar MI sistēmu radīto diskrimināciju. Ar līdzīgām lietam nav saskārusies arī Datu valsts inspekcija kā pamattiesību aizsardzības iestāde datu aizsardzības jomā. Tajā pašā laikā, kā tiks atklāts Pētījumā, citās Eiropas valstīs atbildīgās uzraudzības iestādes jau ir izskatījušas lietas par MI sistēmu radītajiem diskriminācijas riskiem, kā arī sagaidāms, ka līdz ar MI akta spēkā stāšanos un informētību par MI radītajiem riskiem, šādu lietu skaits nākotnē pieaugs.

2. Definīcijas

MI sistēma – mašinizēta sistēma, kura projektēta darboties ar dažādiem autonomijas līmeņiem, kura var pēc ieviešanas būt adaptīva, un kura eksplicītiem vai implicītiem mērķiem secina no informācijas, ko tā saņem, kā ģenerēt iznākumus, piemēram, prognozes, saturu, ieteikumus vai lēmumus, kas var ietekmēt fizisko vai virtuālo vidi.[3]

Nodrošinātājs – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura par samaksu vai par brīvu izstrādā MI sistēmu vai vispārīga lietojuma MI modeli vai kura liek izstrādāt MI sistēmu vai vispārīga lietojuma MI modeli un laiž to tirgū vai nodod MI sistēmu ekspluatācijā ar savu nosaukumu/vārdu vai preču zīmi.

Uzturētājs – fiziska vai juridiska persona, publiskā sektora iestāde, aģentūra vai cita struktūra, kura lieto MI sistēmu, kas ir tās pārziņā, izņemot gadījumus, kad MI sistēmu lieto personiskas neprofesionālas darbības veikšanai.

Biometriskie dati – personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, piemēram, sejas attēli vai daktiloskopiskie dati.

Biometriskā identifikācija – cilvēka fizisko, fizioloģisko, uzvedības vai psiholoģisko īpašību automatizēta atpazīšana nolūkā noskaidrot fiziskas personas identitāti, salīdzinot minētā indivīda biometriskos datus ar datubāzē glabātiem indivīdu biometriskajiem datiem.

Biometriskā verifikācija – automatizēta fizisku personu identitātes verifikācija "viens pret vienu", tostarp autentifikācija, kas notiek, fiziskas personas biometriskos datus salīdzinot ar iepriekš sniegtiem biometriskajiem datiem.

Biometriskās kategorizācijas sistēma – MI sistēma, kuras mērķis ir noteikt fizisku personu piederību konkrētām kategorijām, pamatojoties uz viņu biometriskajiem datiem, ja vien tas nepapildina citus komercpakalpojumus un nav absolūti nepieciešams objektīvu tehnisku iemeslu dēļ.

[3] Šī un pārējās sadaļā sniegtās definīcijas noteiktas MI akta 3. pantā.

Biometriskās tālidentifikācijas sistēma – MI sistēma, kuras nolūks ir identificēt fiziskas personas bez to aktīvas iesaistīšanas, parasti no attāluma salīdzinot personas biometriskos datus ar atsauces datubāzē esošajiem biometriskajiem datiem.

Reāllaika biometriskās tālidentifikācijas sistēma – biometriskās tālidentifikācijas sistēma, kurā biometrisko datu uztveršana, salīdzināšana un identificēšana notiek bez būtiskas aiztures, ieetverot ne tikai tūlītēju identifikāciju, bet arī ierobežotu īslaicīgu aizturi, lai novērstu apiešanu.

Vispārīga lietojuma MI modelis – MI modelis – tostarp, ja šāds MI modelis ir apmācīts ar lielu datu apjomu, izmantojot pašuzraudzību plašā mērogā –, kuram piemīt ievērojams vispārīgums un kurš spēj kompetenti veikt plašu atšķirīgu uzdevumu klāstu neatkarīgi no tā, kādā veidā modelis ir laists tirgū, un kuru var integrēt dažādās lejasposma sistēmās vai lietotnēs, izņemot MI modeļus, ko pirms to laišanas tirgū izmanto pētniecības, izstrādes vai prototipu izstrādes darbībām.

Vispārīga lietojuma MI sistēma – MI sistēma, kura ir balstīta uz vispārīga lietojuma MI modeli, un kam ir spējas kalpot dažādiem mērķiem gan saistībā ar tiešo lietojumu, gan integrēšanu citās MI sistēmās.

3. Mākslīgā intelekta un diskriminācijas aizlieguma tiesiskais regulējums

Šajā sadaļā ir analizēts diskriminācijas aizlieguma, datu aizsardzības un mākslīgā intelekta tiesiskais regulējums ES un Latvijā, kā arī vērsta uzmanību uz esošā tiesiskā regulējuma problēmām un izaicinājumiem algoritmu un MI sistēmu izmantošanas kontekstā.

3.1. Diskriminācijas aizlieguma regulējums

ES diskriminācijas aizlieguma princips ir noteikts kā vispārīgais princips un cilvēka pamattiesības. Diskriminācijas aizliegumu regulē šādi galvenie ES primārie un sekundārie tiesību akti.

Diskriminācijas aizliegums, kā arī sieviešu un vīriešu līdztiesība kā vispārīgie principi ir noteikti Līguma par Eiropas Savienību 2. pantā un 3. panta 2. punktā.[4] Līguma par Eiropas Savienības darbību (LESD) 10. pants paredz, ka, nosakot un īstenojot savu politiku un darbības, ES tiecas apkarot diskrimināciju dzimuma, rases vai etniskās izcelsmes, reliģijas vai pārliecības, invaliditātes, vecuma vai dzimumorientācijas dēļ.[5] LESD 19. panta 1. punkts paredz: "Neskarot pārējos Līgumu noteikumus un nepārsniedzot pilnvaras, ko Savienībai piešķir Līgumi, Padome saskaņā ar īpašu likumdošanas procedūru, saņēmusi Eiropas Parlamenta piekrišanu, ar vien prātīgu lēmumu var paredzēt attiecīgus pasākumus, lai cīnītos pret diskrimināciju dzimuma, rases vai etniskās izcelsmes, reliģijas vai pārliecības, invaliditātes, vecuma vai dzimumorientācijas dēļ."

Atsevišķi LESD noteikumi attiecas uz sieviešu un vīriešu vienlīdzības principu. LESD 8. pants nosaka: "Veicot savas darbības, Savienība tiecas novērst nevienlīdzību starp sievietēm un vīriešiem un sekmēt vienlīdzību." LESD 153. panta 1. punkta i) apakšpunkts paredz, ka sociālās politikas viena no jomām, kurā ES "atbalsta un papildina dalībvalstu darbību" ir "vīriešu un sieviešu vienlīdzība attiecībā uz iespējām darba tirgū un attieksmi darbā". Turklāt LESD 157. pants paredz: "Visas dalībvalstis nodrošina to, lai tiktu ievērots princips, ka vīrieši un sievietes par vienādu vai vienādi vērtīgu darbu saņem vienādu darba samaksu."

Diskriminācijas aizlieguma princips ir noteikts Hartas 21. pantā, kura 1. punkts nosaka: "Aizliegta jebkāda veida diskriminācija, tostarp diskriminācija dzimuma, rases, ādas krāsas, etniskās vai

[4] Līgums par Eiropas Savienību (konsolidētā versija), *OV C* 115/13, 09.05.2008.
[5] Līgums par Eiropas Savienības darbību (konsolidētā versija). *OV C* 326. 26.10.2012.

sociālās izcelsmes, ģenētisko īpatnību, valodas, reliģijas vai pārliecības, politisko vai jebkuru citu uzskatu dēļ, diskriminācija saistībā ar piederību pie nacionālās minoritātes, diskriminācija īpašuma, izcelsmes, invaliditātes, vecuma vai dzimumorientācijas dēļ." Hartas 21. panta 2. punkts savukārt paredz: "Ievērojot Līgumu piemērošanas jomu un neskarot tajos paredzētos īpašos noteikumus, ir aizliegta jebkāda diskriminācija pilsonības dēļ."

Hartā atsevišķi ir paredzēts vīriešu un sieviešu līdztiesības princips. Tās 23. panta 1. punkts nosaka: "Vīriešu un sieviešu līdztiesība ir jānodrošina visās jomās, tostarp nodarbinātības, darba un atalgojuma jomā." Savukārt minētā panta 2. punkts paredz: "Līdztiesības princips neliedz saglabāt vai noteikt pasākumus, kuri paredz īpašas priekšrocības nepietiekami pārstāvētam dzimumam."

Diskriminācijas aizliegumu paredz vairāki turpmāk minētie sekundārie ES tiesību akti. Padomes Direktīva 2000/43/EK, ar ko ievieš vienādas attieksmes principu pret personām neatkarīgi no rasu vai etniskās piederības[6] aizliedz diskrimināciju, pamatojoties uz rasi vai etnisko izcelsmi nodarbinātības, sociālās aizsardzības, tostarp sociālā nodrošinājuma un veselības aprūpes, sociālo priekšrocību, izglītības, preču un pakalpojumu pieejamības un piegādes jomās. Minētā direktīva aizliedz diskrimināciju vienīgi pamatojoties uz rasi vai etnisko piederību kā t.s. aizliegto pamatu, savukārt diskriminācija reliģijas vai pārliecības, invaliditātes, vecuma un dzimumorientācijas dēļ nav aizliegta. Šis likuma robs ir labi zināms cilvēktiesību ekspertu vidū.

Padomes Direktīva 2000/78/EK, ar ko nosaka kopēju sistēmu vienlīdzīgai attieksmei pret nodarbinātību un profesiju[7] aizliedz diskrimināciju, pamatojoties uz vecumu, reliģiju vai pārliecību, invaliditāti un seksuālo orientāciju nodarbinātības jomā. ES direktīvas nosaka diskriminācijas aizliegumu pamatojoties uz dzimumu nodarbinātības, kā arī preču un pakalpojumu jomā: Eiropas Parlamenta un Padomes Direktīva 2006/54/EK par tāda principa īstenošanu, kas paredz vienlīdzīgas iespējas un attieksmi pret vīriešiem un sievietēm nodarbinātības un profesijas jautājumos[8] un Padomes Direktīva 2004/113/EK ar kuru īsteno principu, kas paredz vienlīdzīgu

[6] Padomes Direktīva 2000/43/EK (2000. gada 29. jūnijs), ar ko ievieš vienādas attieksmes principu pret personām neatkarīgi no rasu vai etniskās piederības, OV L 180. 19.7.2000.
[7] Padomes Direktīva 2000/78/EK (2000. gada 27. novembris), ar ko nosaka kopēju sistēmu vienlīdzīgai attieksmei pret nodarbinātību un profesiju, OV L 303, 2.12.2000.
[8] Eiropas Parlamenta un Padomes Direktīva 2006/54/EK (2006. gada 5. jūlijs) par tāda principa īstenošanu, kas paredz vienlīdzīgas iespējas un attieksmi pret vīriešiem un sievietēm nodarbinātības un profesijas jautājumos, OV L 204, 26.7.2006.

attieksmi pret vīriešiem un sievietēm, attiecībā uz pieeju precēm un pakalpojumiem, preču piegādi un pakalpojumu sniegšanu[9].

Algoritmu pieejamība un izmantošana palielina uzņēmumu iespējas detalizēti profilēt lietotājus un mērķtiecīgi piedāvāt potenciāliem klientiem personalizētus piedāvājumus. Tādējādi algoritmiskā diskriminācija, visticamāk, var notikt preču un pakalpojumu tirgū, kur lietotāju uzvedība tiek analizēta un, pamatojoties uz to, tiek noteikti dažādu veidu un cenu piedāvājumi un iespējas. Likumdošanas nepilnības dēļ ES tiesību akti neaizsargā ES pilsoņus pret algoritmisku profilēšanu un mērķauditorijas atlasi preču un pakalpojumu jomā, kas nozīmē, ka noteiktas grupas var tikt izslēgtas no piekļuves noteiktām precēm un pakalpojumiem. Piemēram, varētu rasties situācija, ka diskriminācija rodas, piedāvājot īpaši svarīgas preces un pakalpojumus, piemēram, mājokli, veselību, izglītību utt. Lai gan valsts tiesību akti varētu aizliegt šādus diskriminācijas gadījumus, ES līmenī nav saskaņota aizlieguma. Papildus šai lielajai atšķirībai ES diskriminācijas aizlieguma tiesību materiālajā darbības jomā pastāv arī citi problemātiski izņēmumi, jo īpaši saistībā ar dzimumu līdztiesību. Šie izņēmumi attiecas uz plašsaziņas līdzekļu saturu, reklāmu un izglītību, kas ir izslēgta no Direktīvas 2004/113/EK darbības jomas. Ņemot vērā pieaugošo mākslīgā intelekta izmantošanu attiecīgajās jomās, šie izņēmumi var radīt būtiskas nepilnības, ietekmējot ES tiesību aktu spēju novērst algoritmisko diskrimināciju.[10]

Eiropas Parlamenta un Padomes Direktīvas 2010/41/ES par to, kā piemērot vienlīdzīgas attieksmes principu vīriešiem un sievietēm, kas darbojas pašnodarbinātas personas statusā, un ar kuru atceļ Padomes direktīvu 86/613/EEK[11] 4. pants nosaka vienlīdzīgas attieksmes principu. Minētā panta 1. punkts skaidro, ka tas nozīmē, ka **"**nav nekādas tiešas vai netiešas diskriminācijas dzimuma dēļ publiskā un privātā sektorā, piemēram, saistībā ar uzņēmējdarbības sākšanu, aprīkošanu vai paplašināšanu vai jebkura citāda veida darbību sākšanu vai paplašināšanu pašnodarbinātības jomā".

Viena no ES dzimumu līdztiesības tiesību jomām, kas pakļauta algoritmiskas diskriminācijas riskam, ir vienlīdzīga darba samaksa. Būtiski riski dzimumu līdztiesībai rodas, ja algas noteikšanai (ne)tiešā

[9] Padomes Direktīva 2004/113/EK (2004. gada 13. decembris), ar kuru īsteno principu, kas paredz vienlīdzīgu attieksmi pret vīriešiem un sievietēm, attiecībā uz pieeju precēm un pakalpojumiem, preču piegādi un pakalpojumu sniegšanu, OV L 373, 21.12.2004.

[10] Gerards, J., Xenidis, R. (2021). Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, European Commission.

[11] Eiropas Parlamenta un Padomes Direktīva 2010/41/ES (2010. gada 7. jūlijs) par to, kā piemērot vienlīdzīgas attieksmes principu vīriešiem un sievietēm, kas darbojas pašnodarbinātas personas statusā, un ar kuru atceļ Padomes Direktīvu 86/613/EEK. OV L 180, 15.7.2010.

veidā tiek izmantoti algoritmi, jo īpaši sadarbīgās ekonomikas un platformas darba kontekstā.[12] Esošais tiesiskais regulējums, tai skaitā Direktīva 2010/41/ES efektīvi nerisina "digitālās" dzimumu darba samaksas atšķirības problēmu, jo vienlīdzīgas darba samaksas garantijas neattieksies uz pašnodarbinātajiem platformas darbiniekiem. Tā ir būtiska nepilnība vienlīdzīga darba samaksas principa īstenošanā un galvenais šķērslis ES likumdevēja centieniem novērst darba samaksas atšķirības starp dzimumiem.[13] 2024. gada 24. aprīlī Parlaments pieņēma Platformu darba direktīvu.[14] Saskaņotais teksts būs oficiāli jāpieņem arī Padomei. Pēc tās publicēšanas ES Oficiālajā Vēstnesī dalībvalstīm divu gadu laikā būs jāpārņem direktīvas noteikumi savos tiesību aktos. Jaunie noteikumi paredz, ka personu, kas veic platformas darbu, nevar atlaist, pamatojoties uz algoritma vai automatizētu lēmumu pieņemšanas sistēmas lēmumu. Tā vietā digitālajām darba platformām ir jānodrošina cilvēku pārraudzība pār svarīgiem lēmumiem, kas tieši ietekmē personas, kas veic platformas darbu.

Kā liecina sniegtā analīze, neraugoties uz plašo ES diskriminācijas aizlieguma tiesiskā regulējuma darbības jomu, regulējumam, kas paredz aizsardzību pret diskrimināciju, dzimuma un rases dēļ, ir daudzas nepilnības, kas ir problemātiskas algoritmiskās diskriminācijas kontekstā. Šī situācija ir vēl problemātiskāka attiecībā uz citiem aizsargātiem pamatiem — vecumu, invaliditāti, seksuālo orientāciju un reliģiju —, kuriem saskaņā ar ES tiesību aktiem ir ierobežota aizsardzība.

Līdzās ES regulējumam, diskriminācijas aizlieguma princips ir noteikts daudzos Eiropas Padomes saistošos tiesību aktos, kā arī politikas dokumentos. Eiropas Cilvēktiesību un pamatbrīvībuaizsardzības konvencijas (ECTK)[15] 14. pants paredz, ka konvencijā noteiktās tiesības un brīvības ir īstenojamas bez jebkādas diskriminācijas, neatkarīgi no dzimuma, rases, ādas krāsas, valodas, reliģijas, politiskajiem vai citiem uzskatiem, nacionālās vai sociālās izcelsmes, saistības ar kādu nacionālo minoritāti, mantiskā stāvokļa, kārtas vai cita stāvokļa. ECTK 12. protokols[16] nosaka, ka "jebkuru likumā paredzēto tiesību īstenošana ir nodrošināma bez jebkādas diskriminācijas", sniedzot vēl plašāku aizsargāto pamatu uzskaitījumu, un kas paredz, ka nevienu nevar pakļaut

[12] Gerards, J., Xenidis, R. (2021). Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, European Commission.
[13] Turpat.
[14] Council of the European Union, Proposal for the Directive of the European Parliament and of the Council on improving working conditions in platform work, 8 March 2024, Sk. Parliament adopts Platform Work Directive. News European Parliament, 24-04-2024.
[15] Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.
[16] Eiropas Cilvēktiesību konvencija ar grozījumiem, kas izdarīti ar 11., 14. un 15. protokoliem, iekļaujot protokolus Nr. 1, 4, 6, 7, 12, 13 un 16. (neoficiāls tulkojums)

diskriminācijai no publisko institūciju puses uz jebkāda pamata (1. pants). Latvija šim protokolam nav pievienojusies.

Latvijā diskriminācijas aizlieguma princips ir noteikts Latvijas Republikas Satversmes 91. pantā, kas paredz: "Visi cilvēki Latvijā ir vienlīdzīgi likuma un tiesas priekšā. Cilvēka tiesības tiek īstenotas bez jebkādas diskriminācijas." [17] Satversmes 91. pantā ir ietverti divi savstarpēji cieši saistīti, tomēr dažādi principi: tiesiskās vienlīdzības princips – pirmajā teikumā – un diskriminācijas aizlieguma princips – otrajā teikumā. Šā panta pirmajā teikumā nostiprinātais tiesiskās vienlīdzības princips citstarp liedz valsts institūcijām izdot tādas tiesību normas, kas bez saprātīga pamata pieļauj atšķirīgu attieksmi pret personām, kuras atrodas vienādos un pēc noteiktiem kritērijiem salīdzināmos apstākļos. Savukārt Satversmes 91. panta otrais teikums ir vērsts uz cilvēka tiesību īstenošanu, nepieļaujot diskrimināciju, – tas novērš iespēju, ka demokrātiskā tiesiskā valstī, pamatojoties uz kādu nepieļaujamu kritēriju, piemēram, rasi, tautību vai dzimumu, tiktu ierobežotas personas pamattiesības. Diskriminācijas aizliegums ir tiesiskās vienlīdzības principa palīgelements, kas noteiktos gadījumos šo pricipu precizē un palīdz piemērot konkrētos gadījumos.[18]

Satversmes 91. panta otrajā teikumā ietverts vispārējs diskriminācijas aizliegums, bet nav norādīti tā saucamie nepieļaujamie kritēriji. Par nepieļaujamiem kritērijiem Satversmes tiesas judikatūrā atzīti dzimums, vecums, pilsonība, valoda un tautība, invaliditāte un citi. Šie kritēriji pantā ir "jāielasa", izmantojot tiesību normu interpretācijas metodes, kā arī pamatojoties uz tādu Latvijas tiesību sistēmu raksturojošu principu, ka tā ir atvērta starptautiskajām tiesībām. Līdz ar to uzmanība jāpievērš arī cilvēktiesību attīstības tendencēm pasaulē.[19]

Satversmes tiesa savā judikatūrā arī izšķir **tiešo diskrimināciju**, kad atšķirīga attieksme ir balstīta uz kādu no nepieļaujamiem kritērijiem, un **netiešo diskrimināciju**, kad atšķirīga attieksme var būt balstīta uz neitrālu kritēriju, bet faktiski skart kādu cilvēku grupu, uz kuru šis neitrālais kritērijs

[17] Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). *Latvijas Vēstnesis*, 01.07.1993., Nr. 43.
[18] Latvijas Republikas Satversmes 91. pants. (2022). Tiesiskās vienlīdzības princips. Satversmes tiesas judikatūra. Satversmes tiesa.
[19] Latvijas Republikas Satversmes 91. pants. (2022). Tiesiskās vienlīdzības princips. Satversmes tiesas judikatūra. Satversmes tiesa.

tipiskā veidā attiecas kāda nepieļaujama kritērija dēļ.[20] ES tiesībās līdzīgā veidā tiek izšķirta tiešā un netiešā diskriminācija.[21]

Algoritmiskā diskriminācija rada izaicinājumus robežu noteikšanai starp tiešu un netiešu diskrimināciju. Ņemot vērā grūtības izsekot atšķirīgai attieksmei, kuras pamatā ir nepieļaujamie kritēriji t.s. "melnās kastes" (angļu val. - black box) algoritmos, netiešās diskriminācijas jēdziens varētu kļūt par konceptuālu "patvērumu", lai aptvertu algoritmu diskriminējošās kļūdas. Šāda pieeja varētu mazināt juridisko noteiktību, ja tā "pēc noklusējuma" noved pie atklātās objektīvās pamatojuma pārbaudes vispārināšanas, kas piemērojams netiešās diskriminācijas lietās, pretstatā šaurākajam pamatojumu kopumam, kas piemērojams tiešās diskriminācijas lietās. MI sistēmu pārredzamības un izskaidrojamības problēmas rada arī sarežģītus jautājumus par pierādījumiem, atbildību un uzraudzību.[22]

Diskriminācijas aizliegums ir noteikts daudzos Latvijas tiesību aktos, cita starpā pārņemot arī iepriekš aplūkotās ES direktīvas. 2012. gadā tika pieņemts Fizisko personu — tiesiska darījuma dalībnieku — diskriminācijas aizlieguma likums.[23] Darba likums nosaka vispārīgu atšķirīgas attieksmes aizliegumu visās darba attiecību stadijās, paredzot detalizētāku regulējumu, piemēram, darba intervijā un darba samaksā.[24] Izglītības likuma 3.[1] pants nosaka atšķirīgas attieksmes aizliegums.[25] Līdzīgi arī likuma Par sociālo drošību 2.[1] pants nosaka atšķirīgas attieksmes aizliegumu.[26] Likuma Par policiju 5. panta otrā daļa paredz: **"**Policija aizsargā personu tiesības un likumīgās intereses neatkarīgi no šo personu izcelsmes, dzimuma, vecuma, sociālā un mantiskā stāvokļa, nodarbošanās, pilsonības, rases un nacionālās piederības, attieksmes pret reliģiju, politiskās un citas pārliecības, kā arī izglītības un valodas, dzīvesvietas un citiem apstākļiem."[27] Līdzīgi Operatīvās darbības likuma 4. panta piektā daļa, kas nosaka operatīvās darbības principus, paredz, ka "[o]peratīvās darbības pasākumi veicami neatkarīgi no personu izcelsmes, dienesta un

[20] Turpat.
[21] Sk.European Labour Authority. (2023). Artificial Intelligence and Algorithms in Risk Assessment. Addressing Bias, Discrimination and other Legal and Ethical Issues. A Handbook. Addressing Bias, Discrimination and other Legal and Ethical Issues. A Handbook.
[22] Sk. Gerards, J., Xenidis, R. (2021). Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, European Commission.
[23] Fizisko personu — tiesiska darījuma dalībnieku — diskriminācijas aizlieguma likums. Pieņemts 29.11.2012. *Latvijas Vēstnesis*, 19.12.2012., Nr. 199.
[24] Darba likums. Pieņemts 20.06.2001. *Latvijas Vēstnesis*, 06.07.2001. Nr. 105.
[25] Izglītības likums. Pieņemts 29.10.1998, *Latvijas Vēstnesis*, 17.11.1998., Nr. 343/344.
[26] Par sociālo drošību. Pieņemts 07.09.1995. *Latvijas Vēstnesis*, 21.09.1995., Nr. 144.
[27] Par policiju. Pieņemts 04.06.1991. *Latvijas Republikas Augstākās Padomes un Valdības Ziņotājs*. 15.08.1991, Nr. 31/32.

mantiskā stāvokļa un amata, pilsonības, rases vai etniskās piederības, attieksmes pret reliģiju, politiskajiem uzskatiem un piederības pie politiskajām partijām, sabiedriskajām organizācijām, biedrībām vai citiem apstākļiem. Minētie faktori nedrīkst ietekmēt operatīvo darbību, ja tas nav īpaši norādīts likumā."[28] Administratīvā procesa likuma 6.pants[29] un Kriminālprocesa likuma 8. pants[30] nosaka vienlīdzības principu. Diskriminācijas aizlieguma un vienlīdzības princips ir noteikts arī citos Latvijas tiesību aktos. Tajā pašā laikā minētie noteikumi nav pietiekami, lai efektīvi aizsargātu pret algoritmisko un MI sistēmu radīto diskriminācijas risku.

3.2. Datu aizsardzības regulējums

Papildus tiesiskajam regulējumam, kas attiecas uz diskriminācijas aizliegumu, arī privātuma un datu aizsardzības tiesību aktus var izmantot, lai cīnītos pret algoritmisko diskrimināciju. Lai novērstu algoritmu vai MI sistēmu izmantošanas rezultātā radītos diskriminācijas riskus, būtiska nozīme ir ES datu aizsardzības regulējumam, īpaši Vispārīgajai datu aizsardzības regulai[31] (VDAR).

Datu aizsardzības principi ir piemērojami arī MI sistēmām, kas apstrādā personas datus. VDAR 5. pants kā vienu no personas datu apstrādes principiem nosaka godprātības principu. Saistībā ar godprātības principu var runāt arī par automatizētu lēmumu satura godprātīgumu jeb taisnīgumu (faireness – angļu val.).[32] VDAR 71. apsvērums nosaka: "Lai nodrošinātu godprātīgu un pārredzamu apstrādi attiecībā uz datu subjektu, ņemot vērā konkrētos apstākļus un kontekstu, kurā personas dati tiek apstrādāti, pārzinim būtu jāizmanto piemērotas matemātiskās vai statistikas procedūras profilēšanai, jāveic atbilstīgi tehniski un organizatoriski pasākumi, lai it īpaši nodrošinātu, ka tiek koriģēti faktori, kuru dēļ rodas personas datu neprecizitātes, un ka līdz minimumam ir samazināts kļūdu rašanās risks, jāgarantē personas datu drošība tādā veidā, lai ņemtu vērā iespējamos riskus attiecībā uz datu subjekta interesēm un tiesībām un lai cita starpā novērstu fizisku personu diskrimināciju dēļ rases vai etniskās izcelsmes, politiskajiem uzskatiem, reliģiskās vai ticības piederības, dalības arodbiedrībā, ģenētiskā vai veselības stāvokļa vai dzimumorientācijas, vai izrietošus pasākumus, kas izraisa šādu diskrimināciju. Automatizēta

[28] Operatīvās darbības likums. Pieņemts 16.12.1993, *Latvijas Vēstnesis*, 30.12.1993, Nr. 131.
[29] Administratīvā procesa likums. Pieņemts 25.10.2001, *Latvijas Vēstnesis*, 14.11.2001. Nr. 164.
[30] Kriminālprocesa likums. Pieņemts 21.04.2005, *Latvijas Vēstnesis*, 11.04.2005., Nr. 74.

[31] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). *OV L* 119, 04.05.2016.
[32] Barkane I. (2023). Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, Datu aizsardzība un regulējums masveida novērošanas novēršanai. Rīga: LU Akadēmiskais apgāds.

lēmumu pieņemšana un profilēšana, pamatojoties uz īpašām personas datu kategorijām, būtu jāatļauj tikai saskaņā ar konkrētiem nosacījumiem."

MI sistēmas, kas balstās uz lielu datu apjomu, ļauj pieņemt automatizētus lēmumus, kas arvien plašāk tiek izmantoti arī publiskajā sektorā, to skaitā ir lēmumi, kas pieņemti, izmantojot novērošanas tehnoloģijas un prognozējošos algoritmus sabiedrības drošības un noziedzības apkarošanas interesēs. Policijas direktīva paredz būtisku nosacījumu, ka profilēšana, kas izraisa diskrimināciju pret fiziskām personām, pamatojoties uz īpašu kategoriju personas datiem, ir aizliegta saskaņā ar ES tiesībām (Policijas direktīvas 11. panta 3. punkts).

Profilēšana ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši – analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos (VDAR 4. panta 4. punkts).

Pastāv trīs iespējamie veidi, kā var izmantot profilēšanu. To var izmantot: 1) vispārīgai profilēšanai bez automatizētu lēmumu pieņemšanas; 2) lēmumu pieņemšanai, pamatojoties uz profilēšanu; 3) tikai automatizēta lēmumu pieņemšanai, tostarp profilēšanai, kas rada tiesiskas sekas vai līdzīgā veidā ievērojami ietekmē datu subjektu.

Datu subjektam ir tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu (VDAR 22. panta 1. punkts). Tomēr no šī aizlieguma ir pieļaujami izņēmumi. Saskaņā ar VDAR 21. panta 2. punktu izņēmuma kārtā šāds lēmums var tikt pieņemts, ja tas: 1) ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un datu pārzini; 2) pamatojas uz datu subjekta nepārprotamu piekrišanu; vai 3) ir atļauts saskaņā ar ES vai dalībvalsts tiesību aktiem,kuri ir piemērojami pārzinim un kuros ir arī noteikti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses.

Pirmajos divos gadījumos datu pārzinim jāveic atbilstīgi pasākumi, lai aizsargātu datu subjekta tiesības un brīvības, un leģitīmās intereses – vismaz tiesības panākt cilvēka līdzdalību no pārziņa puses –, lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu (VDAR 22. panta 2. punkts).

Tomēr minētie lēmumi nevar tikt pamatoti ar īpašām personas datu kategorijām, izņemot, ja datu subjekts ir devis nepārprotamu piekrišanu vai apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ, pamatojoties uz ES vai dalībvalsts tiesību aktiem, un tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un leģitīmās intereses (VDAR 22. panta 3. punkts).

Aizsardzības pasākumi automatizētu lēmumu pieņemšanas gadījumā, it sevišķi tad, ja tiek apstrādāti biometriskie dati, ir šādi: tiesības apstrīdēt lēmumu; tiesības panākt cilvēka līdzdalību; tiesības būt informētam par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana; tiesības saņemt jēgpilnu informāciju par automatizētajā lēmumā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu (VDAR 13. panta 2. punkta f) apakšpunkts, 14. a 2. punkta f) apakšpunkts).

Minētās normas paredz informēšanas pienākumu, kas ir saistīts ar vispārīgāku un fundamentālu jautājumu par MI sistēmu un to rezultātu, kā arī ar to saistīto cilvēka pieņemto lēmumu izskaidrojamību. MI sistēmas un to lēmumi ir jāizskaidro. Izskaidrojamība attiecas uz spēju izskaidrot gan sistēmas tehniskos procesus, gan ar tiem saistītos pieņemtos lēmumus. Tehniskā izskaidrojamība prasa, lai MI sistēmas pieņemtos lēmumus varētu saprast cilvēki. Pārredzamības prasības var atklāt, kā šīs sistēmas tiek izmantotas, lai veiktu prognozes, sniegtu ieteikumus vai pieņemtu lēmumus. Tās var atklāt kritērijus, kas ietekmē konkrētu prognozi vai lēmumu. Tomēr ne vienmēr ir iespējams izskaidrot, kāpēc MI sistēma ir pieņēmusi konkrētu rezultātu vai lēmumu un kāda ievades faktoru kombinācija to veicināja. Šos gadījumus dēvē par “melno kasti”. Jaunais ES mākslīgā intelekta regulējuma mērķis ir cita starpā risinātu šos minētos izaicinājumus, kas saistīti ar MI sistēmu pārredzamības un izskaidrojamības prasību nodrošināšanu.

3.3. Eiropas Savienības mākslīgā intelekta regulējums

Lai novērstu MI sistēmu radītos riskus cilvēktiesībām, tai skaitā diskriminācijas riskus, ES ir pieņemts pirmais visaptverošais mākslīgā intelekta regulējums. MI akta mērķis ir uzlabot iekšējā tirgus darbību un veicināt uz cilvēku orientēta un uzticama MI izmantošanu, vienlaikus nodrošinot augstu veselības, drošuma, Hartā nostiprināto pamattiesību, tostarp demokrātijas un tiesiskuma, un vides aizsardzības līmeni pret MI sistēmu radītām kaitīgām sekām ES, un atbalstot inovāciju (1. panta 1. puntkts).

MI akts stājās spēkā 1. augustā, un tas kļūs tieši piemērojamas visās ES dalībvalstīs, tai skaitā Latvijā, pēc diviem gadiem, t.i. no 2026. gada 2. augusta. Tomēr atsevišķiem noteikumiem, ir

paredzēti atšķirīgs piemērošanas termiņš. Piemēram, noteikumi par aizliegtu mākslīgā intelekta (MI) praksi tiks piemēroti pēc 6 mēnešiem, t.i. no 2025. gada 1. februāra, prasības vispārīga lietojuma MI modeļiem - pēc 12 mēnešiem, prasības MI sistēmām, kas ir produkta drošības sastāvdaļa vai ir produkti, uz ko attiecas daži ES saskaņošanas tiesību akti (I pielikums), tiks piemērotas pēc 36 mēnešiem, t.i. no 2027. gada 2. augusta. Savukārt noteikumi par augsta riska MI sistēmām, ko izmanto atsevišķās augsta riska jomās tiks piemēroti, iestājoties MI akta piemērošanas termiņam, proti, pēc 24 mēnešiem.

MI aktā ir uzsvērts, ka tam nevajadzētu ietekmēt praksi, kas ir aizliegta ar ES tiesību aktiem, tostarp tiesību aktiem datu aizsardzības, diskriminācijas novēršanas, patērētāju tiesību aizsardzības un konkurences jomā (45 apsvērums). Tādējādi MI akts nesamazina aizsardzību, ko nosaka esošais diskriminācijas novērošanas tiesiskais regulējums, bet gan papildina esošo regulējumu.

MI akts paredz saskaņotus noteikumus par MI sistēmu laišanu tirgū, nodošanu ekspluatācijā un izmantošanu ES. Tas aizliedz vairākus nepieņemamus MI prakses veidus, kas ir pretrunā ES vērtībām un pamattiesībām, kas nostiprinātas Hartā, ieskaitot tiesības uz nediskriminēšanu. Tas nosaka prasības augsta riska MI sistēmām un pienākumus attiecīgajiem operatoriem, pārredzamības pienākumus attiecībā uz dažām MI sistēmām un saskaņotus noteikumus par vispārīga lietojuma MI modeļu laišanu tirgū. Tas paredz arī uzraudzības un izpildes nodrošināšanas noteikumus.

MI aktā ir izmantota uz risku balstītu pieeja, klasificējot MI sistēmas atkarībā no dažādiem to radītajiem riska līmeņiem. MI klasificēšana kā augsta riska sistēmas ir noteikta MI akta 6. pantā. Pirmkārt, saskaņā ar MI akta 6. panta 1. punktu augstu risku var radīt sistēmas, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas, uz ko attiecas daži ES saskaņošanas tiesību akti, kas uzskaitīti I pielikumā. Tās tiek klasificētas kā augsta riska sistēmas, ja attiecīgajam produktam piemēro atbilstības novērtēšanas struktūras, kas ir trešā persona, veiktu atbilstības novērtēšanas procedūru, ievērojot attiecīgos ES saskaņošanas tiesību aktus. Proti, tādi produkti ir mašīnas, rotaļlietas, lifti, iekārtas un aizsardzības sistēmas, kas paredzētas lietošanai sprādzienbīstamā vidē, radioiekārtas, spiediena iekārtas, atpūtas kuģu aprīkojums, trošu ceļu iekārtas, gāzveida kurināmā iekārtas, medicīniskās ierīces, *in vitro* diagnostikas medicīniskās ierīces, pašgājēji un aviācija (MI akta 51. apsvērums).

Otrkārt, augsta riska MI sistēmas var būt savrupas MI sistēmas, kuras nav produktu drošības sastāvdaļas vai kuras pašas nav produkti. MI akta 6. panta 2. punkts nosaka, ka papildus 6. panta 1. punktā minētajām augsta riska MI sistēmām par augsta riska sistēmām uzskata III pielikumā minētās MI sistēmas. Tās ir klasificējamas kā augsta riska sistēmas, ja, pamatojoties uz to paredzēto nolūku, tās rada augstu kaitējuma risku personu veselībai, drošībai vai pamattiesībām, ņemot vērā gan iespējamā kaitējuma smagumu, gan tā iespējamību, un ja tās lieto vairākās konkrēti noteiktās jomās, kā precizēts MI aktā (MI akta 52. apsvērums).

MI akta III pielikumā ir uzskaitītas astoņas jomas, kurās MI izmantošana rada augstu risku: 1) biometrija, ciktāl to izmantošanu atļauj attiecīgie ES vai valsts tiesību akti; 2) kritiskā infrastruktūara; 3) izglītība un arodmācības; 4) nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai; 5) piekļuve privātiem pamatpakalpojumiem un sabiedriskajiem pamatpakalpojumiem un pabalstiem un to izmantošana; 6) tiesībaizsardzība, ciktāl to izmantošanu atļauj attiecīgie ES vai valsts tiesību akti; 7) migrācijas, patvēruma un robežkontroles pārvaldība, ciktāl to izmantošanu atļauj attiecīgie ES vai valsts tiesību akti; 8) tiesvedība un demokrātijas procesi.

Tajā pašā laikā MI akta III pielikumā minēto MI sistēmu neuzskata par augsta riska sistēmu, ja tā nerada būtisku kaitējuma risku fizisku personu veselībai, drošībai vai pamattiesībām, tostarp būtiski neietekmē lēmumu pieņemšanas iznākumu (MI akta 6. panta 3. punkts). MI sistēma, kas būtiski neietekmē lēmumu pieņemšanas iznākumu, ietver situācijas, kurās ir izpildīts viens vai vairāki turpmāk minētie nosacījumi: a) MI sistēma ir paredzēta šaura procedūras uzdevuma veikšanai; b) MI sistēma ir paredzēta iepriekš pabeigtas cilvēka darbības rezultāta uzlabošanai; c) MI sistēma ir paredzēta lēmumu pieņemšanas modeļu vai noviržu no iepriekšējiem lēmumu pieņemšanas modeļiem atklāšanai, un tā nav paredzēta, lai aizstātu vai ietekmētu iepriekš pabeigtu cilvēka veiktu novērtējumu, bez pienācīgas cilvēka veiktas pārskatīšanas; vai d) MI sistēma ir paredzēta sagatavošanās uzdevuma veikšanai saistībā ar novērtējumu, kas ir būtisks III pielikumā uzskaitīto lietošanas gadījumu nolūkos. Tomēr jebkurā gadījumā MI akta III pielikumā minētu MI sistēmu vienmēr uzskata par augsta riska MI sistēmu, ja MI sistēma veic fizisku personu profilēšanu.

MI akta III pielikumā katrai jomai ir norādīti MI sistēmu lietošanas gadījumi, kas rada augstu risku. Tie tiks aprakstīti Pētījuma nākamajās sadaļās pie konkrētās apskatītās augsta riska jomas. MI akts paredz iespēju, ka Eiropas Komisija groza III pielikumu, pievienojot vai mainot augsta riska MI

istēmu lietošanas gadījumus, ja ir izpildīti divi nosacījumi: a) MI sistēmas ir paredzētas lietošanai jebkurā no III pielikumā uzskaitītajām jomām; b) MI sistēmas rada kaitējuma risku veselībai un drošībai vai nelabvēlīgu ietekmi uz pamattiesībām, un minētais risks ir līdzvērtīgs ar vai lielāks par kaitējuma vai nelabvēlīgas ietekmes risku, ko rada augsta riska MI sistēmas, kuras jau minētas III pielikumā (7. panta 1. punkts).

Lai efektīvi mazinātu riskus veselībai, drošībai un pamattiesībām, MI akts nosaka daudzas obligātas prasības augsta riska MI sistēmām saistībā ar riska pārvaldību (9. pants), izmantoto datu kopu kvalitāti un nozīmīgumu (10. pants), tehnisko dokumentāciju (11. pants) un uzskaiti (12. pants), pārredzamību un informācijas sniegšanu uzturētājiem (13. pants), cilvēka virsvadību (14. pants) un robustumu, precizitāti un kiberdrošību (15. pants) (MI akta 66. apsvērums). Pirms augsta riska MI sistēmas laišanas ES tirgū vai pirms tiek uzsākta citāda šādas sistēmas izmantošana, to nodrošinātājam jāveic MI sistēmas atbilstības novērtēšana**,** lai pārliecinātos, ka to sistēma atbilst minētajām prasībām.

Būtiska nozīme, lai novērstu MI sistēmu izmantošanas radītos diskriminācijas riskus, ir datu kvalitātes un pārvaldības prasībām. MI akta preambula skaidro, ka augstas kvalitātes datiem un piekļuvei šādiem datiem ir būtiska loma daudzu MI sistēmu struktūras un veiktspējas nodrošināšanā, jo īpaši, ja tiek izmantotas metodes, kas ietver modeļu apmācīšanu, ar mērķi nodrošināt, ka augsta riska MI sistēma darbojas, kā paredzēts, un droši un ka tās lietošana nerada diskrimināciju, kas ir aizliegta saskaņā ar ES tiesību aktiem (67. apsvērums). Lai nodrošinātu augstas kvalitātes datu kopas apmācībai, validēšanai un testēšanai, ir jāīsteno atbilstoša datu pārvaldība un pārvaldības prakse. Apmācības, validēšanas un testēšanas datu kopām ir jābūt atbilstošām, pietiekami reprezentatīvām un, cik vien iespējams, bez kļūdām un pilnīgām, ņemot vērā MI sistēmas paredzēto nolūku. Lai veicinātu atbilstību ES datu aizsardzības tiesību aktiem, piemēram, VDAR, datu pārvaldībā un pārvaldības praksē – personas datu gadījumā – ir jāietver pārredzamība attiecībā uz datu vākšanas sākotnējo nolūku. Datu kopām vajadzētu būt arī atbilstošiem statistiskajiem raksturlielumiem, tostarp attiecībā uz personām vai personu grupām, attiecībā uz kurām ir paredzēts lietot augsta riska MI sistēmu. Īpaša uzmanība būtu jāpievērš tādas iespējamās neobjektivitātes mazināšanai datu kopās, kura varētu ietekmēt personu veselību un drošību, kurai varētu būt negatīva ietekme uz pamattiesībām vai kura varētu izraisīt diskrimināciju, kas ir aizliegta ES tiesību aktos, jo īpaši, ja izvaddati ietekmē ievaddatus turpmākām darbībām (atgriezeniskās saites cilpas). Neobjektivitāte, piemēram, var būt raksturīga pamatā esošajām datu kopām, jo īpaši tad, ja tiek izmantoti vēsturiski dati, vai radīta tad, kad sistēmas tiek izmantotas

reālās pasaules apstākļos. MI sistēmu sniegtos rezultātus varētu ietekmēt šāda raksturīga neobjektivitāte, kas tiecas pakāpeniski palielināties un tādējādi turpināt un pastiprināt esošo diskrimināciju, jo īpaši attiecībā uz personām, kas pieder pie dažām neaizsargātām grupām, tostarp rasiskām vai etniskām grupām (MI akta 67. apsvērums).

Pētījuma turpinājumā tiks aplūkoti praktiski piemēri, kā algoritmu un MI sistēmu izmantošana var radīt diskriminācijas riskus četrās no MI akta III pielikuma jomām.

4. Fizisko personu biometriskā identifikācija un kategorizācija

Atbilstoši MI akta III pielikuma 1. punktam, par augsta riska MI sistēmām ir uzskatāmas MI sistēmas, ko izmanto biometrijā, ciktāl to izmantošanu atļauj attiecīgie ES vai valsts tiesību akti šādos trīs lietošanas gadījumos.

Pirmkārt, augstu risku rada biometriskās tālidentifikācijas sistēmas. Tajā pašā laikā ir paredzēta atruna, ka tās neietver MI sistēmas, ko paredzēts izmantot biometriskai verifikācijai, kuras vienīgais nolūks ir apstiprināt, ka konkrēta fiziska persona ir persona, par kuru tā uzdodas.

Otrkārt, augsta riska MI sistēmas ir tādas MI sistēmas, ko paredzēts izmantot biometriskai kategorizēšanai pēc sensitīviem vai aizsargātiem atribūtiem vai raksturlielumiem, pamatojoties uz minēto atribūtu vai raksturlielumu inferenci. Biometriskā kategorizācija nozīmē fizisku personu iedalīšana konkrētās kategorijās, pamatojoties uz viņu biometriskajiem datiem. Šādas konkrētas kategorijas var būt saistītas ar tādiem aspektiem kā dzimums, vecums, matu krāsa, acu krāsa, tetovējumi, personības iezīmes, valoda, reliģija, piederība nacionālajai minoritātei, seksuālā vai politiskā orientācija. Tas neietver biometriskās kategorizācijas sistēmas, kas ir tikai papildfunkcija, kura ir cieši saistīta ar citu komercpakalpojumu, proti, tas nozīmē, ka objektīvu tehnisku iemeslu dēļ šo funkciju nevar izmantot bez galvenā pakalpojuma (MI akta 16. apsvērums).

Treškārt, augstu risku rada arī MI sistēmas, ko paredzēts izmantot emociju atpazīšanai.

MI sistēmas, ko izmanto biometrijas jomā, ir uzskatāmas par augsta riska sistēmām, ja vien tās nav klasificējamas kā aizliegtas MI sistēmas saskaņā ar ES vai valstu tiesību aktiem.

MI akts paredz vairākus aizliegtas MI prakses veidus (5. pants). Cita starpā arī iepriekš minētās trīs MI sistēmas biometrijas jomā var tikt klasificēta kā aizliegta MI prakse.

MI akts aizliedz MI sistēmu laišanu tirgū, nodošanu ekspluatācijā šim konkrētajam mērķim vai lietošanu fiziskas personas emociju izsecināšanai darbavietā vai izglītības iestādēs, izņemot tad, ja MI sistēmas izmantošanu paredzēts ieviest vai laist tirgū medicīnisku vai drošības iemeslu dēļ (5. panta 1. punkta pirmās daļas g) punkts).

MI akts daļēji aizliedz arī biometrisko kategorizāciju. Proti, ir aizliegta tādu biometriskās kategorizācijas sistēmu laišana tirgū vai nodošana ekspluatācijā, vai lietošana, kuras individuāli kategorizē fiziskas personas, pamatojoties uz viņu biometriskajiem datiem, lai atvedinātu vai

izsecinātu viņu rasi, politiskos uzskatus, dalību arodbiedrībās, reliģiskos vai filozofiskos uzskatus, dzimumdzīvi vai seksuālo orientāciju. Šis aizliegums neattiecas uz likumīgi iegūtu biometrisko datu kopu, piemēram, attēlu, marķēšanu vai filtrēšanu, pamatojoties uz biometriskajiem datiem, vai biometrisko datu kategorizēšanu tiesībaizsardzības jomā (MI akta 5. panta 1. punkta pirmās daļas g) punkts).

Uz biometrisko kategorizāciju attiecas vēl viens MI aktā noteiktais aizliegums. MI akts aizliedz arī MI sistēmas laišanu tirgū, nodošanu ekspluatācijā šim konkrētajam mērķim vai lietošanu fizisku personu radītā riska novērtējuma veikšanai, lai novērtētu vai prognozētu risku, ka fiziska persona varētu izdarīt noziedzīgu nodarījumu, kura balstās vienīgi uz fiziskas personas profilēšanu vai uz tās personisko īpašību un rakstura iezīmju novērtēšanu. Šo aizliegumu nepiemēro MI sistēmām, kuras izmanto, lai atbalstītu cilvēka veiktu novērtējumu par personas iesaistīšanos noziedzīgā darbībā, kurš jau ir balstīts uz objektīviem un pārbaudāmiem faktiem, kas ir tieši saistīti ar noziedzīgu darbību (MI akta 5. panta 1. punkta pirmās daļas d) punkts).

Pārējos gadījumos, kad uz biometriskajām kategorizācijas sistēmām nav attiecināms aizliegums, šīs sistēmas ir uzskatāmas par augsta riska sistēmām.

MI aktu aizliedz arī reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu publiski piekļūstamās vietās tiesībaizsardzības nolūkos (MI akta 5. panta 1. h) punkts). Tajā pašā laikā no šī aizlieguma ir paredzēti vairāki izņēmumi. Proti, šādu sistēmu izmantošana ir aizliegta, izņemot tad, ja – un tiktāl, cik – tāda izmantošana ir absolūti nepieciešama kādam no šiem mērķiem:
i) konkrētu nolaupīšanas, cilvēku tirdzniecības vai cilvēku seksuālas izmantošanas upuru mērķtiecīga meklēšana, kā arī bezvēsts pazudušu personu meklēšana; ii) konkrēta, būtiska un nenovēršama apdraudējuma fizisku personu dzīvībai vai fiziskai drošībai vai reālu un pašreizēju vai reālu un paredzamu teroristu uzbrukuma draudu novēršana; iii) par noziedzīga nodarījuma izdarīšanu aizdomās turētas personas atrašanās vietas noteikšana vai personas identificēšana nolūkā veikt kriminālizmeklēšanu vai kriminālvajāšanu vai kriminālsoda izpildi par II pielikumā minētajiem nodarījumiem, par kuriem attiecīgajā dalībvalstī var piemērot brīvības atņemšanas sodu vai ar brīvības atņemšanu saistītu drošības līdzekli, kura maksimālais ilgums ir vismaz četri gadi (MI akta 5. panta 2. punkta pirmā daļa).

MI akts paredz detalizētus noteikumus, lai nodrošinātu, ka minēto biometriskās tālidentifikācijas sistēmu iepriekš norādītajās izsmeļošajās jomās izmantošana ir atbildīga, samērīga un tiesiska (5. panta 2.-7. punkts). Katrā no izsmeļoši uzskaitītajām situācijām ir jāņem vērā daži elementi, it īpaši

situācijas raksturs, kurš pamato sistēmas lietošanu, lietošanas ietekme uz visu attiecīgo personu tiesībām un brīvībām, un saistībā ar lietošanu paredzētie aizsardzības pasākumi un nosacījumi. Turklāt reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski piekļūstamās vietās tiesībaizsardzības nolūkos būtu jāizvērš tikai, lai apstiprinātu konkrētas personas identitāti, un tai būtu jānotiek tikai tiktāl, cik tas ir absolūti nepieciešams laikposma, kā arī ģeogrāfiskā un personiskā tvēruma ziņā, jo īpaši, ņemot vērā pierādījumus vai norādes par draudiem, cietušajiem vai nodarījuma izdarītāju. Reāllaika biometriskās tālidentifikācijas sistēmu lietošana publiski piekļūstamās vietās būtu jāatļauj vienīgi tad, ja attiecīgā tiesībaizsardzības iestāde ir pabeigusi novērtējumu par ietekmi uz pamattiesībām, ja vien MI aktā nav paredzēts citādi, un ir reģistrējusi sistēmu ES datubāzē (5. panta 2. punkta otrā daļa, 34. apsvērums).

Katrai biometriskās tālidentifikācijas sistēmu izmantošanai ir nepieciešama iepriekšēja atļauja, ko izsniegusi tiesu iestāde vai neatkarīga administratīva iestāde (5. panta 3. punkts, 35. apsvērums). Dalībvalsts var paredzēt iespēju pilnīgi vai daļēji atļaut reāllaika biometriskās tālidentifikācijas sistēmu izmantošanu publiski piekļūstamās vietās tiesībaizsardzības nolūkos, ievērojot ierobežojumus un nosacījumus, kas uzskaitīti MI aktā. Šādā gadījumā dalībvalstij savos tiesību aktos ir jānosaka noteikumus par atļauju pieprasīšanu, izsniegšanu un izmantošanu, kā arī ar tām saistīto uzraudzību un ziņošanu. Dalībvalstis var ieviest ierobežojošākus tiesību aktus par biometriskās tālidentifikācijas sistēmu lietošanu (MI akta 5. panta 5. punkts).

MI sistēmu lietošana fizisku personu reāllaika biometriskajai tālidentifikācijai publiski piekļūstamās vietās tiesībaizsardzības nolūkos neizbēgami ietver biometrisko datu apstrādi. MI akta noteikumi, kas aizliedz (ar dažiem izņēmumiem) šādu lietošanu un pamatojas uz LESD 16. pantu ir piemērojams kā lex specialis attiecībā uz Direktīvas (ES) 2016/680 (Policijas direktīvas) 10. panta noteikumiem par biometrisko datu apstrādi, tādējādi izsmeļoši regulējot šādu lietošanu un ar to saistīto biometrisko datu apstrādi (38. apsvērums).

MI akts paredz, ka MI aktā ietvertais reāllaika biometriskās tālidentifikācijas sistēmu izmantošanas aizliegums neskar VDAR 9. pantu attiecībā uz biometrisko datu apstrādi nolūkos, kas nav tiesībaizsardzība (5. panta 1. punkta otrā daļa). Biometrisko datu un citu personas datu apstrādei saistībā ar MI sistēmu lietošanu biometriskajai identifikācijai, kas nav saistīta ar reāllaika biometriskās tālidentifikācijas sistēmu lietošanu publiski piekļūstamās vietās tiesībaizsardzības nolūkos, kā to reglamentē MI akts, arī turpmāk ir jāatbilst visām prasībām, kas izriet no Direktīvas (ES) 2016/680 (Policijas direktīvas) 10. panta. Nolūkos, kas nav tiesībaizsardzība, VDAR 9. panta 1.

punkts aizliedz biometrisko datu apstrādi, ievērojot tajā paredzētos izņēmumus. Piemērojot VDAR 9. panta 1. punktu, uz biometriskās tālidentifikācijas lietošanu nolūkos, kas nav tiesībaizsardzība, jau attiecās valsts datu aizsardzības iestāžu lēmumi par aizliegšanu (39. apsvērums). Savukārt, gadījumos, kad šādas sistēmas nav aizliegtas, tās ir uzskatāmas par augsta riska MI sistēmām.

Turpmāk tiks aplūkoti konkrēti prakses piemēri, kas parāda kā šīs sistēmas var radīt diskriminācijas risku. Turpmākā analīze neietver izvērtējumu par šo sistēmu klasificēšanu.

Prakses piemēri

Dienvidvelsas policija prettiesiski izmanto reāllaika sejas atpazīšanu publiskās vietās

Viena no lietām, kurā tika izvērtēta algoritmiskā neobjektivitāte un tās tiesiskais regulējums, bija saistīta ar Dienvidvelsas policijas reāllaika sejas atpazīšanas tehnoloģijas izmantošanu.[33] Kopš 2017. gada Dienvidvelsas policija vairākas reizes izmēģināja reāllaika sejas atpazīšanu publiskās vietās, kas radīja bažas par privātuma pārkāpumiem un iespējamu neobjektivitāti sistēmā. Šo izmēģinājumu veikšana tika apstrīdēta tiesā. Lieta tika ierosināta, pamatojoties uz pilsonisko brīvību aizstāvja Eda Bridžesa (Ed Bridges) prasību.

2020. gada 11. augustā Apvienotās Karalistes Apelācijas tiesa atzina, ka sejas atpazīšanas tehnoloģijas izmantošana ir nelikumīga. Tiesa konstatēja, ka, pirmkārt, ir pārkāptas ECTK 8. pantā noteiktās tiesības uz privātumu. Otrkārt, spriedumā tika konstatēts, ka Dienvidvelsas policija nav pienācīgi izvērtējusi, vai tās izmēģinājumiem varētu būt diskriminējoša ietekme, un, jo īpaši, tā neveica saprātīgus pasākumus, lai noteiktu, vai tās izmantotā sejas atpazīšanas programmatūra nerada neobjektīvitātes **rases vai dzimuma dēļ**. Tiesa konstatēja, ka tādējādi policija nav izpildījusi pienākumus saskaņā ar publiskā sektora vienlīdzības pienākumu, kas izriet no Vienlīdzības likuma.

Jāņem vērā, ka šajā gadījumā nebija pierādījumu, ka konkrētais algoritms būtu neobjektīvs, taču Dienvidvelsas policija neveica saprātīgas darbības, lai to izvērtētu. No sprieduma izriet, ka publiskā sektora iestādēm, ir jāveic saprātīgi pasākumi, lai izvērtētu potenciālās neobjetivitātes, izvietojot algoritmiskās sistēmas, un lai pastāvīgi atklātu algoritmiskās neobjektivitātes.

[33] Sk. Simons & Simons. (2 September, 2020). UK Court of Appeal finds facial recognition technology unlawful; Centre for Data Ethics and Innovation. (2020). Review into bias in algorithmic decision-making; Sabbagh, D. (11 August, 2020). South Wales police lose landmark facial recognition case. *The Guardian.*

Jānorāda, ka Dienvidvelsas policija atsāka sejas atpazīšanas tehnoloģijas izmantošanu pēc ziņojuma, ko tā pasūtīja kopā ar Metropolitēna policiju. Ziņojumā tika konstatēts, ka rases un dzimuma atšķirības ir minimālas, ja tehnoloģija tiek izmantota, izvēloties noteiktus iestatījumus. Par to bažas ir paudušas cilvēktiesību aizstāvības organizācija Liberty.[34] Dienvidvelsas policijas mājaslapā ir aprakstīts, kādā veidā tā izmanto sejas atpazīšanas tehnoloģijas.[35]

Kembridžas Universitātes pētījums par Apvienotās Karalistes sejas atpazīšanas tehnoloģiju izmantošanu policijas darbā

2022. gada oktobrī Kembridžas Universitātes Minderoo Tehnoloģiju un demokrātijas centra (Minderoo Centre for Technology and Democracy) pētnieki izveidoja audita rīku, lai novērtētu sejas atpazīšanas tehnoloģiju atbilstību tiesiskajam regulējumam un vadlīnijām.[36] Cita starpā tika izvērtēta atbilstība Apvienotās Karalistes datu aizsardzības un vienlīdzības tiesību aktiem, kā arī tiesu spriedumiem un pilsoniskās sabiedrības organizāciju un Informācijas komisāra biroja (Information Commissioner's Office) paustajiem viedokļiem. Tika izvērtēta atbilstība arī tādām pamattiesībām kā privātums, vienlīdzība, diskriminācijas aizliegums, vārda un pulcēšanās brīvība.

Pētnieki izvērtēja trīs sejas atpazīšanas tehnoloģiju izmantošanu Apvienotās Karalistes policijā. Viena no tām bija saistīta ar iepriekš minēto tiesas lietu, kurā Kārdifā dzīvojošs pilsonisko brīvību kampaņas dalībnieks apstrīdēja Dienvidvelsas policijas automatizētas sejas atpazīšanas tehnoloģijas izmantošanu, lai reāllaikā pārbaudītu cilvēkus un salīdzinātu sejas ar noziedzīgu nodarījumu izdarījušo personu "uzraudzības sarakstā". Pētnieki pārbaudīja arī līdzīgus Metropolitēna policijas veiktus reāllaika sejas atpazīšanas tehnoloģiju izmantošanas izmēģinājumus. Trešā tehnoloģija, kas tika pārbaudīta, bija sejas atpazīšanas lietotne viedtālruņos, ko izmantoja Dienvidvelsas policijas darbinieki, lai skenētu pūļus, lai reāllaikā identificētu "meklētās personas".

Pētījums atklāja, ka visos trīs gadījumos policijas sejas atpazīšanas tehnoloģiju izmantošana neatbilst minimālajiem ētiskajiem un juridiskajiem standartiem. Pamatojoties uz atklājumiem, kas

[34] BBC. (8 April 2023). Facial recognition tech: Liberty 'police racism' claim.
[35] South Wales Police. Facial Recognition Technology.
[36] Radiya-Dixit, E. (2022). A Sociotechnical Audit: Assessing Police Use of Facial Recognition; Sk. arī Minderoo Centre for Technology and Democracy. (2022). A Sociotechnical Audit: Assessing Police use of Facial Recognition; University of Cambridge. (27 October, 2022). UK police fail to meet 'legal and ethical standards' in use of facial recognition.

publicēti ziņojumā, eksperti pievienojās aicinājumiem aizliegt policijai izmantot sejas atpazīšanu publiskās vietās.

Pētījumā ir norādīts, ka līdzās riskiem, ko sejas atpazīšanas tehnoloģiju izmantošana rada privātumam un pulcēšanās brīvībai, tās rada arī bažas par diskrimināciju. Pētnieki norāda, ka vēsturiski novērošanas sistēmas tiek izmantotas marginalizētu grupu uzraudzībai, un jaunākie pētījumi liecina, ka pati tehnoloģija satur raksturīgu neobjektivitāti, kas nesamērīgi nepareizi identificē sievietes, cilvēkus ar tumšu ādas krāsu un cilvēkus ar invaliditāti.

Visos trijos gadījumos tika atklāts pārredzamības trūkums. To izmantošana netika pārredzami novērtēta attiecībā uz tehnoloģiju aizspriedumiem vai diskrimināciju tās lietošanā. Piemēram, Metropolitēna policija pirms reāllaika sejas atpazīšanas izmēģinājumiem nepublicēja novērtējumu par tehnoloģijas rasu vai dzimuma aizspriedumiem. Svarīga informācija par policijas sejas atpazīšanas tehnoloģiju izmantošanu tiek "aizsargāta", tostarp demogrāfiskie dati, kas publicēti par arestiem vai citiem rezultātiem, tādējādi apgrūtinot izvērtēšanu, vai rīki “atspoguļo” rasu profilēšu. Pētījums arī atklāja, ka trūkst skaidrs un efektīvs kompensācijas mehānisms personām un kopienām, kurām ir nodarīts kaitējums policijas izmantoto tehnoloģiju dēļ.[37]

Sejas atpazīšanas tehnoloģijas izmantošana ASV un diskriminācijas pamatojoties uz rasi

2020. gadā Amerikas Savienoto Valstu (ASV) ziņās tika pievērsta uzmanība policijas izmeklēšanai Detroitā, kurā bija iesaistīts Roberts Viljamss (Robert Williams).[38] Afroamerikānis Viljamss tika arestēts par zādzību veikalā, pamatojoties uz sejas atpazīšanas identifikāciju. Viņš tika aizturēts trīsdesmit stundas un pēc drošības naudas iemaksāšanas atbrīvots. Vēlāk tika atzīts, ka atbilstība, ko konstatēja sejas atpazīšanas tehnoloģija, balstoties uz personas autovadītāja apliecības fotogrāfiju, bija nepatiesa. Policijas departaments atvainojās un ierosināja pārskatīt sejas atpazīšanas tehnoloģijas izmantošanu. Viljamss uzsāka tiesvedību pret policiju, pieprasot kompensāciju.[39]

Šis gadījums parāda risku, ka aizdomās turēto identificēšanai tiek izmantota neprecīza tehnoloģija un uz to paļaujas, veicot aizturēšanu. Viljamsa gadījums ir viens no vairākiem līdzīgiem piemēriem

[37] Radiya-Dixit, E. (2022). A Sociotechnical Audit: Assessing Police Use of Facial Recognition.
[38] Smith, M., Mann, M. (2024). Facial Recognition Technology and Potential for Bias and Discrimination. In: Matulionyte R, Zalnieriute M, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge Law Handbooks. Cambridge University Press, p. 87-95.
[39] Harwell, D. (13 April 2021). Wrongfully arrested man sues Detroit police over false facial recognition match. Washington Post.

no visas ASV, kas ir pievērsis uzmanību rasu aizspriedumiem saistībā ar sejas atpazīšanu, ko saasina minoritāšu pārmērīgā pārstāvība policijas datubāzēs.

Policijas datubāzēs esošā mazākumtautību grupu, piemēram, melnādaino vīriešu, pārāk liela pārstāvība nozīmē, ka tās, visticamāk, tiks identificētas, izmantojot sejas atpazīšanu. Datubāzēs iekļautos sejas attēlus var izmantot arī sejas atpazīšanas tehnoloģiju analīzē. Atkarībā no konkrētajiem izmantošanas gadījumiem (t.i., not tā, kā tehnoloģija tiek izmantota un izmantotajiem novērošanas sarakstiem), ir pamats uzskatīt, ka sejas atpazīšanas tehnoloģija vērš policiju pret tām personām, kuras viņiem jau ir zināmas.

ASV pētījumi par sejas atpazīšanas neobjektivitāti rases un dzimuma dēļ

ASV ir veikti daudzi empīriski pētījumi par sejas atpazīšanas tehnoloģiju neobjektivitāti, pamatojoties uz rasi.[40] Pētījumi atklāj uz datiem balstītus iemeslus, kāpēc mazākumtautību grupas var tikt pakļautas nepareizai vai pārmērīgai identifikācijai, izmantojot sejas atpazīšanas tehnoloģiju. 2019. gadā Nacionālā standartu un tehnoloģiju institūta (NIST) ziņojumā tika norādīts, ka sejas atpazīšanas tehnoloģijai bija ievērojami zemāks precizitātes līmenis, atpazīstot afroamerikāņu un aziātu sejas — faktiski tika konstatēts, ka šo rasu sejām ir no 10 līdz 100 reižu lielāka iespēja tikt nepareizi identificētām, salīdzinot ar balto vīriešu sejām.[41] Citā pētījumā, ir atklāts, ka tumšādaino sieviešu nepareizas identifikācijas rādītājs ir aptuveni 35 procenti, kas ir piecdesmit reizes lielāks nekā baltajiem vīriešiem.[42]

ASV sejas atpazīšanas tehnoloģiju datubāzēs, kurās lielākoties ir baltādainu un vīriešu dzimuma personu attēli, ietver aizspriedumus pret tumšādainiem cilvēkiem. Sistēmai var būt lielāka kļūdas iespēja attiecībā uz citas ādas krāsas un sieviešu dzimuma personām.[43] Tādējādi šādu grupu pārstāvji var biežāk tikt diskriminēti, piemēram, daudz biežāk nepamatoti apstādināti vai aizturēti.

---

[40] Sk. Barkane I. (2023). Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, Datu aizsardzība un regulējums masveida novērošanas novēršanai. Rīga: LU Akadēmiskais apgāds.
[41] Grother, P., Ngan, M., Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology.
[42] Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91.
[43] Hardesty, L. (11 February, 2018). Study finds gender and skintype bias in commercial artificial intelligence systems. *Massachusetts Institute of Technology.*

ASV veiktajos pētījumos ir paustas bažas, ka šādas tehnoloģijas var tikt izmantotas, lai kontrolētu un izsekotu visvairāk marginalizētās kopienas un vēl vairāk atstumtu un diskriminētu noteiktas etniskās grupas, kurām jau tāpat ir pievērsta pastiprināta valsts iestāžu uzmanība.[44]

Pieņemot algoritmiskos lēmumus, kas saistīti ar datu izmantošanu, diskriminācija var rasties dažādu iemeslu dēļ – to var radīt aizspriedumi, kas apzināti vai neapzināti ir iekļauti sejas atpazīšanas algoritma izveides, testēšanas un ieviešanas laikā, kā arī lēmumi, kādas darbības veikt, pamatojoties uz iegūtajiem rezultātiem. MI sistēmu rezultātus būtiski ietekmē algoritmu vai programmatūras izstrādē izmantoto datu kvalitāte, kas var atspoguļot neobjektivitāti, neprecizitātes un kļūdas datu vākšanas procesā.[45] Nepareizas identifikācijas iemesls ir datu ievade, uz kuru paļaujas algoritmi, kas pārbauda atbilstību. Ir konstatēts, ka vidēji datu kopās, ko izmanto algoritmu apmācībai, ir aptuveni 80 procenti personu ar gaišāku ādas krāsu.[46] Tāpēc neprecizitāti izraisa pārstāvība datu kopās, ko izmanto, lai izveidotu un apmācītu algoritmus. Tehnoloģiju izstrādātājiem ir jāņem vērā rasu pārstāvība datu kopās, ko izmanto, lai apmācītu sejas atpazīšanas algoritmus. Ja šo problēmu neizdosies novērst, proaktīvi veicot pasākumus, lai sejas atpazīšanas tehnoloģiju datu kopās iekļautu reprezentatīvu pārstāvību, tas varētu būt rasisma veids neatkarīgi no tā, vai tas ir darīts apzināti vai neapzināti.[47] Ir daudz pierādījumu tam, ka biometriskās atpazīšanas tehnoloģijas izmantošana var izraisīt diskrimināciju, jo īpaši ādas krāsas un dzimuma dēļ, ja algoritma vai pamatā esošās datu kopas neobjektivitāte netiek pietiekami novērsta.[48]

Lai sejas atpazīšanas programmatūra būtu efektīva un precīza, tā "jāapmāca" ar lielu daudzumu sejas attēlu. Jo vairāk sejas attēlu, jo precīzākas prognozes. Turklāt precizitāti nosaka ne tikai apstrādāto sejas attēlu daudzums, bet arī to kvalitāte. Datu kvalitātei nepieciešams arī seju attēlu kopums, kas ietver dažādas cilvēku grupas. Tomēr daudzos gadījumos algoritmu izveidei tiek vairāk izmantoti baltādaino vīriešu sejas attēli, mazāk – sieviešu un citas etniskās izcelsmes personu

[44] Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute*.
[45] FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement.
[46] Turpat
[47] Smith M., Mann M. (2024). Facial Recognition Technology and Potential for Bias and Discrimination. In: Matulionyte R, Zalnieriute M, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge Law Handbooks. Cambridge University Press, p. 87-95.
[48] Sk. Council of Europe, CAHAI. (2020). Feasibility Study; FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement; Gentzel, M. (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. *Philosophy & Technology,* 34, p. 1639–1663; Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute*; Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91.; Grother, P., Ngan, M., Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology.

attēli. Tāpēc sejas atpazīšanas sistēmas labi darbojas attiecībā uz baltādainiem vīriešiem, bet ievērojami sliktāk tās atpazīst melnādainos iedzīvotājus un sievietes.[49] Salīdzinot personu sejas attēlu ar attēliem datubāzē vai novērošanas sarakstā, ir lielāka kļūdas iespējamība jeb t. s. kļūdaini pozitīvie (false positive – angļu val.) gadījumi.

MI uzraudzības sistēmas var radīt negatīvu ietekmi arī uz mazāk aizsargātām grupām, piemēram, bērniem, veciem cilvēkiem un cilvēkiem ar invaliditāti. Sejas atpazīšanas precizitāte attiecībā uz bērniem ir ievērojami zemāka.[50] Kļūdainas atbilstības risks palielinās, ja jaunībā uzņemtus sejas attēlus izmanto salīdzināšanai pēc vairāk nekā pieciem gadiem. Tas pats attiecas uz vecāku cilvēku sejas attēliem. Laiks starp attēla uzņemšanu un tā salīdzināšanu negatīvi ietekmē sejas atpazīšanas tehnoloģiju precizitāti.[51]

Sejas atpazīšanas tehnoloģijas var veikt ne tikai personas identificēšanu, bet arī biometrisko verifikāciju, kā arī līdzeklis, lai veiktu biometrisko kategorizēšanu. Biometriskās kategorizēšanas sistēmas, kuru pamatā ir fizisku personu biometriskie dati, piemēram, personas seja vai pirkstu nospiedumi, lai izsecinātu personas politiskos uzskatus, dalību arodbiedrībās, reliģisko pārliecību vai filozofisko pārliecību, rasi, dzimumdzīvi un seksuālo orientāciju, ir aizliegtas, ņemot vērā, ka tās ir īpaši aizskarošas attiecībā uz plašu klāstu personu tiesībām un brīvībām. Tās aizskar personu pamattiesības, tai skaitā cilvēka cieņu, privātumu un diskriminācijas aizlieguma principu, veicinot sistemātiskus sabiedrības aizspriedumus un rasismu, kā arī ir plaši kritizētas, jo tām trūkst zinātnisku pierādījumu.[52]

[49] Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91.
[50] Michalski, D., Yiu, S. Y., Malec, C. (2018). The impact of age and threshold variation on facial recognition algorithm performance using images of children, *2018 International Conference on Biometrics* (*ICB*), pp. 217–224.
[51] FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement.
[52] Sk. Joint civil society amendments to the Artificial Intelligence Act. Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorization.

5. Izglītība un arodapmācības

MI sistēmām var būt nozīmīga loma, lai paplašinātu piekļuvi izglītībai. Tomēr MI sistēmu izmantošana izglītības jomā var arī radīt nevienlīdzības un diskriminācijas risku. MI straujā attīstība pārveido izglītību vēl nebijušā tempā, piedāvājot jaunas iespējas personalizēt mācību pieredzi, atbalstīt skolotājus viņu ikdienas uzdevumu veikšanā, palielināt darba produktivitāti un optimizēt izglītības pārvaldību.[53]

MI sistēmu ieviešana izglītībā ir svarīga, lai veicinātu kvalitatīvu digitālo izglītību un apmācību un lai visi izglītojamie un skolotāji varētu apgūt un dalīties ar nepieciešamām digitālām prasmēm un kompetencēm, tostarp medijpratību un kritisko domāšanu, lai aktīvi piedalītos ekonomikas, sabiedrības un demokrātiskajos procesos. Tomēr MI sistēmas, ko lieto izglītībā un arodmācībās, MI aktā ir klasificētas kā augsta riska MI sistēmas, jo tās var noteikt izglītības vai profesionālo ievirzi personas dzīvē un tādējādi varētu ietekmēt minētās personas spēju nodrošināt sev iztiku. Ja šādas sistēmas ir nepareizi projektētas un tiek neatbilstīgi lietotas, tās var būt īpaši aizskarošas un var pārkāpt tiesības uz izglītību un apmācību, kā arī tiesības uz nediskriminēšanu un nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, pret sievietēm, noteiktām vecuma grupām, personām ar invaliditāti vai personām ar noteiktu rases vai etnisko izcelsmi vai dzimumorientāciju (MI akta 56. apsvērums).

Saskaņā ar MI akta III pielikuma 3. punktu augstu risku rada turpmāk minētās četru veidu MI sistēmas, ko izmanto izglītībā un arodmācībā. Pirmkārt, augstu risku rada MI sistēmas, ko paredzēts izmantot, lai noteiktu fizisku personu piekļuvi izglītības un arodmācību iestādēm visos līmeņos vai viņu iestāšanos tajās vai viņu uzņemšanu tajās. Otrkārt, par augsta riska MI sistēmām ir uzskatāmas tādas MI sistēmas, ko paredzēts izmantot, lai izvērtētu mācību rezultātus, tostarp, ja šos rezultātus izmanto, lai vadītu fizisku personu mācību procesu izglītības un arodmācību iestādēs visos līmeņos. Treškārt, augstu risku rada MI sistēmas, ko paredzēts izmantot, lai novērtētu pienācīgu izglītības līmeni, kuru persona saņems vai kuram tā varēs piekļūt izglītības un arodmācības iestādēs vai saistībā ar tām visos līmeņos. Ceturtkārt, augstu risku rada MI sistēmas, ko paredzēts izmantot, lai pārbaudījumu laikā izglītības un arodmācības iestādēs vai saistībā ar tām uzraudzītu un konstatētu audzēkņu neatļautu uzvedību visos līmeņos.

[53] Sk. The World Bank. (2024). AI Revolution in Education. What You Need to Know.

MI akts ir noteikts arī viens aizliegums, kas tieši attiecas uz izglītības jomu. Konkrētāk, MI akts aizliedz tādu MI sistēmu laišanu tirgū, nodošanu ekspluatācijā vai lietošanu, kuras paredzēts lietot, lai noteiktu personu emocionālo stāvokli situācijās, kas saistītas ar darba vietu un izglītību. Minētais aizliegums neattiecas uz MI sistēmām, kas laistas tirgū tikai un vienīgi medicīnisku vai drošības iemeslu dēļ, piemēram, uz sistēmām, kas paredzētas lietošanai terapeitiskos nolūkos (5. panta 1. punkta pirmās daļas f) punkts). Ir nopietnas bažas par tādu MI sistēmu zinātnisko pamatojumu, kuru mērķis ir identificēt vai izsecināt emocijas, jo īpaši tāpēc, ka emociju izpausmes dažādās kultūrās un situācijās un pat vienas personas gadījumā ievērojami atšķiras. Šādu sistēmu galvenie trūkumi ir ierobežotā uzticamība, specifiskuma trūkums un ierobežotā vispārināmība. Tāpēc MI sistēmas, kas identificē vai izsecina fizisku personu emocijas vai nodomus, pamatojoties uz to biometriskajiem datiem, var radīt diskriminējošus rezultātus un var aizskart attiecīgo personu tiesības un brīvības. Ņemot vērā nevienlīdzīgo spēku samēru darba vai izglītības jomā un to, ka šīs sistēmas pēc būtības ir aizskarošas, šādas sistēmas varētu izraisīt kaitējošu vai nelabvēlīgu attieksmi pret konkrētām fiziskām personām vai to grupām (MI akta 44. apsvērums).

Turpmāk ir minēti vairāki uzskatāmi piemēri no ārvalstu prakses, kas parāda, kā MI sistēmu izmantošana izglītības jomā var būt diskriminējoša un tādējādi radīt būtisku kaitējumu studentiem.

Prakses piemēri

Tiešsaistes eksāmenu uzraudzības programmatūra

Nīderlandes Cilvēktiesību institūts (College voor de Rechten van de Mens) izskatīja lietu par krāpšanas apkarošanas programmatūras lietošanu Amsterdamas Brīvajā Universitātē (Vrije Universiteit Amsterdam, Nīderlande). Lēmums sniedz būtiskas atziņas par algoritmu kontroli.[54] Krāpšanas programmatūras apkarošanas lietā studente jutās diskriminēta sistēmas dēļ, kas tika izmantota tiešsaistes eksāmenu kārtošanai universitātē. Viņa piedzīvoja tehniskas problēmas eksāmena laikā, jo, pēc viņas domām, programmatūra neatpazina viņas seju tumšās ādas krāsas dēļ. Nīderlandes Cilvēktiesību institūta galīgais lēmums lietā bija tāds, ka konkrētajā gadījumā nebija pierādāma diskriminācija. Augstskola parādīja, ka studentei eksāmenu laikā nebija vairāk problēmu kā citiem studentiem un ka problēmas nav izraisījusi viņas ādas krāsa. Tomēr Nīderlandes Cilvēktiesību institūts uzsver, ka šādu sistēmu vai lietojumprogrammu izmantošana citos gadījumos var izraisīt diskrimināciju. Lieta arī parāda, ka personām ir svarīgi zināt, ka tās

[54] Dutch Data Protection Authority. (2024). AI & Algorithmic Risks Report Netherlands. Report winter 2023/2024.

saskaras ar MI sistēmu vai algoritmiem, lai viņas varētu apstrīdēt jebkuru rezultātu vai prasīt atbildību par šādu sistēmu izmantošanu.

Ir zināms, ka sejas atpazīšanas programmatūras var būt neobjektīvas un novest pie diskriminācijas **rases un dzimuma dēļ**.[55] Minētais piemērs liecina, ka to izmantošana tiešsaistes eksāmenu programmatūras nodrošināšanai izglītības iestādēs var negatīvi ietekmēt apstākļus, kādos studenti kārto eksāmenus un pat viņu spēju tos nokārtot, piemēram, ja programmatūra nespēj atpazīt tumšādainus studentus. Šādas programmatūras izmantošana var negatīvi ietekmēt arī **skolēnus ar invaliditāti**, piemēram, radot trauksmi, neļaujot viņiem tikt aprūpētiem vai neļaujot skolēniem atpūsties no datora.[56] Ģimenēm ar **zemiem ienākumiem**, kur ģimenes locekļiem mājās nav atsevišķas istabas vietas trūkuma dēļ, pārbaudes programmatūras izmantošana var radīt nelabvēlīgus apstākļus, signalizējot par "neatbilstošu uzvedību", ja tiek identificēti ģimenes locekļi, kas iet garām ekrānam.

Diskriminējošas programmas MI radīta teksta noteikšanai

Stenfordas Universitātes pētnieku pētījums, kas tika veikts 2023. gadā, atklāja iepriekš neievērotu problēmu mākslīgā intelekta radīta satura, piemēram, Chat GPT detektoros — tie bieži nepareizi klasificē tekstu, ko rakstījuši cilvēki, kuriem angļu valoda nav dzimtā, kā MI radītu.[57]

Pētījumā tika novērtēti vairāki biežāk lietotie ģeneratīvu iepriekš apmācītu transformatoru (GPT) detektori, izmantojot datu kopu, kurā bija 91 TOEFL esejas, ko rakstījuši studenti, kuriem angļu valoda nav dzimtā valoda, un 88 esejas, ko rakstījuši angļu valodā runājošie ASV studenti. Rezultāti liecināja, ka GPT detektoriem bija augsts viltus pozitīvu rezultātu rādītājs, kas vairāk nekā 50% esejas, ko sarakstījuši ārvalstu studenti, nepareizi atzīmēja kā MI rakstītas. Šīm esejām bija mazāka lingvistiskā mainība un paredzamība, līdzīgi kā MI radītajam tekstam. Turpretim detektori parādīja gandrīz ideālu precizitāti esejās, ko rakstīja ASV studenti.

Pēc pētnieku domām, statistikas rādītāji, ko izmanto daudzi GPT detektori, **netieši diskriminē personas, kurām angļu valoda nav dzimtā** un kurām tādējādi ir ierobežots vārdu krājums un

[55] Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91.
[56] Sk. Brown, L. X. Z. (16 November, 2020). How Automated Test Proctoring Software Discriminates Against Disabled Students. Centre for Democracy and Technology.
[57] Liang, W., Yuksekgonul, M., Mao, Y. et al. (2023). GPT detectors are biased against non-native English writers, *Patterns*, 4 (7); Sk. Myers, A. (15 May, 2023). AI-Detectors Biased Against Non-Native English Writers. Stanford Institute for Human-Centered Artificial Intelligence; Sample, I. (10 July, 2023). Programs to detect AI discriminate against non-native English speakers, shows study. *The Guardian*.

gramatikas lietojums. Lai parādītu šo neobjektivitāti, pētnieki izmantoja valodas modeli, lai uzlabotu vārdu krājumu esejās, kuras sarakstījuši ārvalstu studenti, padarot tās daudzveidīgākas. Šī iejaukšanās ievērojami samazināja nepareizas klasifikācijas skaitu, parādot lingvistisko faktoru ietekmi uz detektora veiktspēju.

Pētījuma rezultātiem ir nopietna ietekme uz rakstniekiem un citiem teksta satura veidotājiem, kuriem angļu valoda nav dzimtā valoda, kuri var saskarties ar nepamatotām apsūdzībām par krāpšanu vai plaģiātismu akadēmiskā un profesionālā vidē, kurās tiek izmantoti GPT detektori. Pētnieki brīdina par nekontrolētu šo rīku izmantošanu vērtēšanas kontekstā, jo pastāv liels risks sodīt tos, kuriem angļu valoda nav dzimtā valoda.

Pētnieki iesaka vispusīgi novērtēt GPT detektorus, izmantojot dažādas datu kopas, un rūpīgi apsvērt to lietošanu. Pētījumā uzsvērta nepieciešamība izstrādāt taisnīgākas un stingrākas MI sistēmu noteikšanas metodes, kas nerada kaitīgus aizspriedumus. Tas aicina uz iekļaujošu publisku diskusiju par MI izmantošanu rakstīšanā un politikas veidošanu, kas ievēro visu autoru tiesības.

Kopumā pētījums vērš izmanību uz pašreizējo GPT detektoru trūkumiem un to potenciālu saasināt diskrimināciju. Tas uzsver, ka ir steidzami jārisina šīs problēmas, lai novērstu dažādu iedzīvotāju grupu marginalizāciju un nodrošinātu godīgumu MI sistēmās. Rezultāti, iespējams, veicinās turpmāku darbu, lai uzlabotu GPT noteikšanas tehnoloģiju pārredzamību, precizitāti un godīgumu.

Tādējādi izglītības iestādēm, izmantojot MI sistēmas, lai pārbaudītu, vai studenti izmanto MI satura radīšanai, ir jāņem vērā, ka arī šādas sistēmas var radīt riskus, piemēram, kā iepriekš minētajā gadījumā, tās var būt diskriminējošas pret tiem, kuriem angļu valoda nav dzimtā valoda vai kas to pārvalda sliktāk.

Algoritmu izmantošana eksāmenu vērtēšanā

Ņemot vērā COVID-19 situāciju, Apvienotajā Karalistē valdības nolēma 2020. gada vasarā atcelt skolas eksāmenus un aizstāt tos, atrodot alternatīvu pieeju atzīmju piešķiršanai.[58] Visā Apvienotajā Karalistē tika mēģināts īstenot līdzīgus procesus, lai to panāktu. Proti, līdzās skolotāju vērtējumam, tika izmantots arī algoritms, lai standartizētu rezultātus, izmantojot statistiskos datus, kas

[58] Centre for Data Ethics and Innovation. (2020). Review into bias in algorithmic decision-making; Kippin, S., Cairney, P. (2022). The COVID-19 exams fiasco across the UK: four nations and two windows of opportunity. *British Politics*, 17, p. 1–23.

mēģināja panākt līdzīgu atzīmju sadalījumu kā iepriekšējos gados. Pieeja tika mainīta, reaģējot uz sabiedrības bažām un kritiku gan par individuālo godīgumu, gan bažām, ka vērtējumi ir neobjektīvi.

MI sistēmu izmantošana uzņemšanai augstskolās

2020. gadā Teksasas Universitātes Ostinā Datorzinātņu nodaļa atteicās no mašīnmācīšanās programmas, ko tā izmantoja, lai novērtētu pretendentus uz doktora studiju programmu. Programmas datubāze savā algoritmā izmantoja iepriekšējos uzņemšanas lēmumus, un kritiķi apgalvoja, ka ir samazinātas iespējas studentiem no dažādām vietām.[59]

2013. gadā Teksasas Universitātes Ostinā Datorzinātņu fakultāte sāka izmantot mašīnmācības sistēmu ar nosaukumu GRADE, lai palīdzētu pieņemt lēmumus par to, kurus no pretendentiem uzņemt doktora studiju programmā. GRADE, kas apzīmē absolventu uzņemšanas vērtētājs (angļu val. – GRADUATE Admissions Evaluator) izveidoja universitātes mācībspēks, lai sākotnēji palīdzētu katedras absolventu uzņemšanas komitejai ietaupīt laiku. GRADE prognozēja, cik liela ir iespēja, ka uzņemšanas komisija apstiprinās pretendentu, un izsaka šo prognozi kā skaitlisku punktu skaitu no pieciem. Sistēma arī izskaidro, kādi faktori visvairāk ietekmēja tās lēmumu.

Universitātes pētnieki, kas izveidoja GRADE, apmācīja to, izmantojot datubāzi ar pagātnes uzņemšanas lēmumiem. Sistēma izmanto šo lēmumu modeļus, lai aprēķinātu kandidātu punktu skaitu. Piemēram, ieteikuma vēstules, kurās ir vārdi "labākais", "balva", "pētniecība" vai "doktorantūra", var novest pie augstāka rezultāta, savukārt vēstules, kas satur vārdus "labi", "klase", "programmēšana" vai "tehnoloģija", norāda uz noraidīšanu. Augstāks vidējais vērtējums nozīmē, ka pretendents, visticamāk, tiks pieņemts, tāpat kā elitārās koledžas vai universitātes nosaukums CV. Sistēmas ietvaros iestādes tika iekodētas kategorijās "elite", "laba" un "cita", pamatojoties uz Datorzinātņu fakultātes aptauju.

Katru lietojumprogrammu GRADE, kas iegūta septiņu gadu laikā, kad tā tika izmantota, joprojām pārskatīja vismaz viens cilvēku komitejas loceklis. Pirms GRADE ieviešanas, mācībspēki veica vairākas pārskatīšanas reizes. Sistēma ietaupīja komitejas laiku, pēc tās izstrādātāju domām, ļaujot mācībspēkiem koncentrēties uz pretendentiem, kas atrodas uzņemšanas vai noraidīšanas slieksnī, un pārskatīt pretendentus dilstošā kvalitātes secībā. 2012. un 2013. gada pieteikšanās sezonā izstrādātāji rakstā par savu darbu norādīja, ka tas samazināja katra kandidāta pilno atsauksmju

[59] Burke, L. (13 December, 2020). The Death and Life of an Admissions Algorithm. *Inside Higher Ed*.

skaitu par 71 % un kopējo failu pārskatīšanas laiku par 74 %. Laikā no 2000. līdz 2012. gadam pieteikumi uz datorzinātņu doktorantūras programmu pieauga no aptuveni 250 līdz gandrīz 650, lai gan mācībspēku skaits, kas varēja izskatīt šos pieteikumus, lielākoties palika nemainīgs. 2012. gadā pieteikumu skaits sasniedzis virs 1200.

Teksasas Universitātē vairākus gadus izvairījās no uzmanības pievēršanas programmatūras izmantošanai. 2020. gadā Merilendas Universitātes fizikas nodaļa Kolokvija parkā rīkoja sarunu ar diviem GRADE radītājiem. Saruna ieguva uzmanību Twitter, jo maģistrantūras studenti apsūdzēja GRADE veidotājus par nelabvēlīgu situācijas radīšanu nepietiekami pārstāvētām grupām (sievietām, melnādainajiem, latīņamerikāņiem) uzņemšanas procesā.

Jau sen pastāv bažas par iespējamību, ka mašīnmācīšanās algoritmi var ietekmēt cilvēku aizspriedumus vai tos saasināt. Algoritmi tiek apmācīti ar datiem. Konkrētajā gadījumā, šie dati atspoguļoja vēsturiskas nevienlīdzības rezultātu. Lai gan ASV daudzām **sievietēm, melnādainiem un latīņamerikāņiem** ir bijusi veiksmīga karjera datorzinātnēs, šīs grupas šajā jomā kopumā ir nepietiekami pārstāvētas. GRADE veidotāji apgalvoja, ka sistēma ir ieprogrammēta tikai tā, lai atkārtotu to, ko uzņemšanas komisija darīja pirms 2013. gada, nevis pieņemtu labākus lēmumus nekā cilvēki. Sistēma nav ieprogrammēta tā, lai prognozēšanai **izmantotu rasi vai dzimumu**. Pretēji tam tika izteikta kritika, ka rasi un dzimumu var iekodēt citās sistēmas izmantotās lietojumprogrammas funkcijās. Sieviešu koledžas un universitātes, kurās vēsturiski mācās melnādainie, var būt nepietiekami novērtētas ar algoritmu. Ir zināms, ka ieteikuma vēstules atspoguļo dzimumu aizspriedumus, jo ieteikuma sniedzējas studentes biežāk raksturo kā "gādīgas", nevis "pārliecinošas".

Pārsteigumu radīja fakts, ka nav tikušas veiktas nekādas darbības, lai pārbaudītu GRADE programmatūras darbību un ietekmi, piemēram, to, kā rezultāti atšķiras dažādās demogrāfiskajās grupās.

2021. gadā tehnoloģiju ziņu portāls The Markup izpētīja konsultāciju firmas EAB konsultāciju programmatūru Navigate, ko plaši izmanto lielas ASV universitātes. Viņi atklāja, ka **melnādainajiem studentiem** ir noteikts četras reizes "augstāks risks" nepabeigt izvēlēto

specialitāti nekā baltādainajiem studentiem. Tādējādi izglītības konsultanti var mudināt melnādainos, latiņu un pamatiedzīvotāju studentus neizvēlēties noteiktas specialitātes.[60]

Viens no iespējamiem uzlabojumiem varētu būt sociālo kategoriju, piemēram, **rases un dzimuma**, "attīrīšana" no datiem, no kuriem algoritmi mācās. Tomēr sociālo kategoriju datu izslēgšana ne vienmēr padara algoritmu mazāk neobjektīvu. Sociālie identifikatori ir tik plaši izplatīti, ka mašīnmācīšanās algoritmi var atklāt citus modeļus datos, kas atklāj dzimumu vai rasi, piemēram, sociālos sakarus vai adreses.[61]

Neobjektivitātes iespēja MI modeļos ir viena no lielākajām problēmām saistībā ar MI sistēmu izmantošanu izglītībā.[62] Datu kopas tiek izmantotas, lai apmācītu algoritmus, un, ja šajās datu kopās ir ietverta neobjektīva informācija, MI sistēma var netīši pastiprināt un palielināt šos aizspriedumus. Piemēram, datu kopu, kas atspoguļo skolotāju netiešos aizspriedumus, kuri sākotnēji vērtēja uzdevumus, var izmantot, lai apmācītu uz MI balstītu vērtēšanas sistēmu. Tas var nostādīt dažas studentu grupas negodīgā nelabvēlīgā situācijā. Līdzīgi arī MI sistēmas, kas iesaka kursus vai karjeras izvēli, var būt neobjektīvas par labu noteiktām demogrāfiskajām grupām, ja apmācību datos ir ietverti sabiedrības aizspriedumi un stereotipi, radot nevienlīdzību.

Viena no būtiskām problēmām ir iespējama neobjektivitāte MI algoritmos, ko izmanto studentu profilēšanai. Algoritmi var atspoguļot un iemūžināt izglītības sistēmā esošus aizspriedumus, piemēram, **rases vai dzimuma dēļ**. Piemēram, ja mākslīgā intelekta sistēma ir apmācīta uz vēsturiskiem datiem, kas atspoguļo aizspriedumus, piemēram, vērtēšanā, tā var negodīgi nostādīt neizdevīgākā situācijā noteiktas studentu grupas.

Apskatītie prakses gadījumu liecina, ka MI sistēmu un algoritmu iespējamās negatīvās sekas ne vienmēr ir viegli izvērtējamas. Izglītības iestādēm būtu jānodrošina, ka studenti ir informēti par to, kā tiek izmantoti viņu dati, un viņiem ir iespēja atteikties no profilēšanas, izmantojot MI sistēmas. Turklāt MI algoritmi ir regulāri jāpārbauda, lai noteiktu neobjektivitāti un taisnīgumu, un jāveic atbilstoši korektīvi pasākumi, lai mazinātu jebkādas konstatētās novirzes.

---

[60] Feathers, T. (2 March, 2021). Major Universities Are Using Race as a "High Impact Predictor" of Student Success. The Markup.

[61] Wood, M. (2021). What are the Risks of Algorithmic Bias in Higher Education? *Every Learner Everywhere.*

[62] Yahaya, A., Habu, J., Sani A. et al. (2024). Examining the Potential Misuse of Artificial Intelligence in Education. *Proceedings of the International Conference on Multidisciplinary Aspect of AI and IOT for Sustainable National Development*.

6. Nodarbinātība, darba ņēmēju pārvaldība un piekļuve pašnodarbinātībai

MI sistēmas, kuras lieto nodarbinātībā, darba ņēmēju pārvaldībā un piekļuvē pašnodarbinātībai, jo īpaši personu darbā līgšanā un atlasē, lēmumu pieņemšanā, kas skar darba attiecību, paaugstināšanas amatā un darba līgumattiecību izbeigšanas kārtību, uzdevumu sadalē, pamatojoties uz individuālo uzvedību vai personības iezīmēm vai īpašībām, un darba līgumattiecībās esošu personu pārraudzībā vai izvērtēšanā, var ievērojami ietekmēt karjeras iespējas nākotnē, minēto personu labklājību un darba ņēmēju tiesības. Tāpēc MI akts klasificē minētās sistēmas kā augsta riska sistēmas. Minētās sistēmas var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, attiecībā uz sievietēm, dažām vecuma grupām, personām ar invaliditāti vai personām ar noteiktu etnisko vai rasisko piederību vai seksuālo orientāciju. MI sistēmas, ko lieto šādu personu snieguma un uzvedības pārraudzībai, var arī apdraudēt viņu pamattiesības uz datu aizsardzību un privātumu (MI akta 57. apsvērums).

MI akta III pielikums nosaka, ka augstu risku rada divu veidu MI sistēmas, ko izmano nodarbinātības, darba ņēmēju pārvaldības un piekļuves pašnodarbinātībai jomās (4. punkts). Pirmkārt, augstu risku rada MI sistēmas, ko paredzēts izmantot fizisku personu pieņemšanai darbā vai darbinieku atlasei, jo īpaši, lai izvietotu mērķtiecīgus darba sludinājumus, analizētu un atsijātu darba pieteikumus un izvērtētu kandidātus. Otrkārt, par augsta riska MI sistēmām uzskatāmas tādas sistēmas, ko paredzēts izmantot, lai pieņemtu lēmumus, kas skar darba attiecību, paaugstināšanas amatā vai darba līgumattiecību izbeigšanas kārtību, sadalītu uzdevumus, pamatojoties uz individuālo uzvedību vai personības iezīmēm vai īpašībām, vai lai pārraudzītu un izvērtētu darba līgumattiecībās esošo personu sniegumu un uzvedību.

Līdzīgi kā izglītības jomā, MI akts aizliedz tādu MI sistēmu laišanu tirgū, nodošanu ekspluatācijā vai lietošanu, kuras paredzēts lietot, lai noteiktu personu emocionālo stāvokli situācijās, kas saistītas ar darba vietu. Minētais aizliegums neattiecas uz MI sistēmām, kas laistas tirgū tikai un vienīgi

medicīnisku vai drošības iemeslu dēļ, piemēram, uz sistēmām, kas paredzētas lietošanai terapeitiskos nolūkos (5. panta 1. punkta pirmās daļas f) punkts). Ņemot vērā nevienlīdzīgo spēku samēru darba jomā un to, ka šīs sistēmas pēc būtības ir aizskarošas, šādas sistēmas varētu izraisīt kaitējošu vai nelabvēlīgu attieksmi pret konkrētām fiziskām personām vai to grupām (MI akta 44. apsvērms).

Turpmāk ir minēti vairāki uzskatāmi piemēri no ārvalstu prakses, kas parāda, kā MI sistēmu izmantošana nodarbinātības jomā var pārkāpt diskriminācijas aizlieguma principu.

Prakses piemēri

Amazon darbā pieņemšanas algoritms

Reuters 2018. gadā publicēja informāciju, ka, Amazon atteicās no MI personāla atlases rīka, kas bija **diskriminējoša pret sievietēm**.[63] Amazon ir viens no lielākajiem tehnoloģiju uzņēmumiem pasaulē, kas plaši izmanto mašīnmācības un mākslīgā intelekta sistēmas. 2015. gadā Amazon atklāja, ka algoritms, kas tika izmantots darbinieku pieņemšanai darbā, ir neobjektīvs pret sievietēm. Algoritms tika balstīts uz pēdējo desmit gadu laikā iesniegto CV skaitu, un, tā kā lielākā daļa pretendentu bija vīrieši, tas tika apmācīts dot priekšroku vīriešiem, nevis sievietēm. Sistēma deva priekšroku vīriešu kandidātiem, noraidot CV, kuros bija iekļauts vārds "sieviete", kā arī pazemināja sieviešu koledžu absolventu reitingus. Mēģinājumi uzlabot algoritmu, padarot to neitrālāku, nenovērsa diskriminējošo iznākumu, jo sistēma varēja secināt dzimumu no citiem datiem.[64]

Darba meklēšanas platforma Nīderlandē

Pētnieki no Utrehtas Universitātes sadarbojās ar darba meklēšanas platformu, lai izpētītu, kā **valodas lietojums atkarībā no dzimuma,** meklējot sludinājumus, sniedz atšķirīgus rezultātus ar diskriminējošu informācijas sadalījumu par darba iespējām.[65]

[63] Dastin, J. (11 October, 2018). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters.*
[64] European Labour Authority. (2023). Artificial Intelligence and Algorithms in Risk Assessment. Addressing Bias, Discrimination and other Legal and Ethical Issues. A Handbook.
[65] van Es, K., Everts, D., Muis, I. (2021). Gendered language and employment Web sites: How search algorithms can cause allocative harm, *First Monday*, 26 (8).

Darba sludinājumu izplatīšana, izmantojot sociālo mediju platformas

Tiešsaistes mērķtiecīga darba sludinājumu izplatīšana, ko nodrošina sociālo mediju platformas, piemēram, Facebook, piedāvātie optimizācijas pakalpojumi, arī veicina **dzimumu** stereotipus, kā arī dzimumu segregāciju darba vietā.[66] AlgorithmWatch 2020. gadā veikts eksperiments parādīja, ka Facebook izplatot reklāmas "neitrāli" (nemērķējot uz konkrētu auditoriju), reklāma par kravas automašīnas vadītāja amatu tika rādīta sabiedrībai, kurā 93% bija vīrieši un 7% sievietes. Un otrādi, sludinājums par pedagoga amatu izplatīta auditorijai, kuru veido 96% sieviešu un 4% vīriešu. [67]

Sejas atpazīšanas un emociju analīzes sistēmas personāla atlasē

Uz mākslīgo intelektu balstītas sejas atpazīšanas un emociju uztveršanas sistēmas var izraisīt diskrimināciju **rases dēļ** vai nostādīt nelabvēlīgā situācijā darba **kandidātus ar invaliditāti**. Tas ir saistīts ar šādu ierīču zemāku precizitātes līmeni attiecībā uz sejas attēliem ar tumšāku ādas krāsu, īpaši **sievietēm**.[68] Turklāt emociju analīzes programmatūra, kas apmācīta atpazīt neiroloģiskus traucējumus, var nedarboties pareizi. Tā kā ar mākslīgo intelektu balstīta emociju analīze arvien vairāk tiek izmantota personāla atlases sektorā, piemēram, lai analizētu darba kandidātu prezentāciju videoierakstus, tas varētu radīt piekļūstamības un iekļaušanas problēmas. Kā iepriekš minēts, MI akts aizliedz izmantot emociju uztveršanas sistēmas darbā un izglītības iestādēs.

Platformu darbinieku diskriminācija

Algoritmus arvien vairāk izmanto arī, lai noteiktu sadarbīgās ekonomikas darbinieku atalgojumu atkarībā no piedāvājuma un pieprasījuma, kvalitātes rādītājiem, darbinieku pieejamības utt. Jo īpaši vairāki faktori, ko ņem vērā šie algoritmi, var negatīvi ietekmēt **dzimumu līdztiesību, nosakot atalgojumu**.[69] Platformas bieži mudina lietotājus novērtēt saņemto pakalpojumu. Klientu diskriminējoši uzskati var ietekmēt platformas darbinieku darba apstākļus, kas cita starpā rada zemāku atalgojumu un mazāk labvēlīgus darba apstākļus vai pat darba zaudēšana. Piemēram,

---

[66] Ali, M., Sapiezynski, P., Bogen, M. et al. (2019). Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes, *Proceedings of the ACM on Human-Computer Interaction*, 3.

[67] Wulf, J. (2022). Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected, *AlgorithmWatch*; Kayser-Bril, N. (2020). Automated Discrimination: Facebook uses gross stereotypes to optimize ad delivery, *AlgorithmWatch*.

[68] Sk. Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91.; Devlin, H. (16 February, 2020). AI systems claiming to 'read' emotions pose discrimination risks. *The Guardian*.

[69] Gerards, J., Xenidis, R. (2021). Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, European Commission.

pasažieru diskriminējoši dzimumu stereotipi var negatīvi ietekmēt Uber sieviešu autovadītāju atalgojumu, pazeminot viņu reitingu, tādējādi negatīvi ietekmējot to, cik daudz braukšanas pieprasījumu viņas saņem, izmantojot Uber lietotni. Papildus diskriminējošiem klientu vērtējumiem, algoritmi, ko izmanto atalgojuma noteikšanai, var arī ņemt vērā tādus kritērijus kā platformas darbinieku pieejamība darbam, viņu reakcijas laiks uz klientu prasībām, vidējais laiks, ko viņi pavada, veicot uzdevumu utt. Sievietēm var būt mazāk iespēju strādāt elastīgu darba laiku pēc pieprasījuma, ja viņām ir jāsavieno darbs ar ģimenes un bērnu aprūpes pienākumiem. Barzilay un Ben-David pētījums par platformas darbu liecina, ka platformas darbinieku sieviešu vidējie stundas ienākumi ir tikai divas trešdaļas no vīriešu stundas algas.[70] Ja atalgojuma noteikšanai izmantotajā algoritmā tiek ņemta vērā elastība vai pieejamība, tas var ietekmēt iznākumu un izraisīt dzimumu nevienlīdzību.

Platformu darbinieki var tikt diskriminēti arī citos veidos. Pret uzņēmumu Uber Eats tika iesniegtas daudzas prasības par kompensāciju par **diskriminācijuu rases** dēļ no autovadītājiem, kas, apgalvojot, ka ir nepatiesi atlaisti sejas atpazīšanas tehnoloģijas darbības traucējumu dēļ.[71] 2024. gadā Uber Eats autovadītājs saņēma finansiālu atlīdzību pēc šādas prasības iesniegšanas.[72] Viņš apgalvoja, ka sejas atpazīšanas programmatūra, kas tika izmantota, lai piekļūtu darba lietotnei, bija "rasistiski neobjektīva". Piekļuve lietotnei bija nepieciešama, lai iegūtu darbu un atalgojumu, tomēr autovadītājs, kas ir melnādains, vairākkārt saskārās ar grūtībām verifikācijas pārbaudēs, kurās tika izmantoti MI sistēma un automatizēti procesi. Viņš bija strādājis par Uber Eats autovadītāju Oksfordšīrā kopš 2019. gada novembra. 2021. gadā viņš tika neatgriezeniski dzēsts no platformas pēc neveiksmīgas sejas atpazīšanas pārbaudes, jo pastāvēja “neatbilstība”. Autovadītājs iesniedza savas prasības darba tiesā; tomēr Uber iesniedza pieteikumu, lai viņa prasības tiktu noraidīta vai tiktu piespriests depozīts, lai viņš varētu to turpināt. Pieteikums tika noraidīts pēc tiesas sēdes 2022. gadā, kurā Uber apgalvoja, ka Manjang konts ir deaktivizēts, jo tika atkārtoti atzīmēts kā neparasta lietotnes lietošana. Lietas finansējumu nodrošināja Vienlīdzības un cilvēktiesību komisija un Lietotņu autovadītāju un kurjeru savienība (App Drivers & Couriers Union), kas paziņoja, ka ir nobažījusies par MI izmantošanu un to, kā to varētu izmantot, lai neatgriezeniski apturētu piekļuvi lietotnei un tādējādi atņemtu ienākumus autovadītājam.

[70] Barzilay, A.R., Ben-David, A. (2017). Platform Inequality: Gender in the Gig-Economy. Seton Hall Law Review: Vol. 47 (2).
[71] Butler S. (2021). Uber facing new UK driver claims of racial discrimination. *The Guardian.*
[72] Jackson I. (2024). Uber Eats worker wins payout over ‘racist’ AI facial recognition – what can HR learn? *People Management*.

Minētie prakses piemēri norāda, ka svarīgi ir nodrošināt, lai veids, kādā tiek izstrādātas MI sistēmas ir pārredzams un lai pirms jaunu MI sistēmu lietošanas, tiktu veikts risku novērtējums. Ieviešot jaunas MI sistēmas, uzņēmumiem ir jāievēro īpaša piesardzība, izvērtējot vai sistēmā izmantotie algoritmi nerada diskriminācijas risku.

7. Piekļuve privātiem pamatpakalpojumiem, sabiedriskajiem pakalpojumiem un pabalstiem un to izmantošana

Vēl viena joma, kurā MI sistēmu lietošanai ir jāpievērš īpaša uzmanība, ir piekļuve dažiem privātiem un sabiedriskiem pamatpakalpojumiem un pabalstiem, kas cilvēkiem nepieciešami, lai viņi varētu pilnvērtīgi piedalīties sabiedrības norisēs vai uzlabot savu dzīves līmeni, un šādu pakalpojumu un pabalstu izmantošana.

Saskaņā ar MI akta III pielikumu augstu risku rada turpmāk minētās MI sistēmas, ko izmanto piekļuves privātiem pamatpakalpojumiem un sabiedriskajiem pamatpakalpojumiem un pabalstiem un to izmantošana turpmāk minētajās četrās jomās (5. punkts).

Pirmkārt, par augsta riska MI sistēmām ir uzskatāmas tādas MI sistēmas, ko paredzēts izmantot publiskajās iestādēs vai to vārdā, lai izvērtētu fizisku personu tiesības saņemt pamata sociālās palīdzības pabalstus un pakalpojumus, tostarp veselības aprūpes pakalpojumus, kā arī lai piešķirtu, samazinātu, atsauktu vai atgūtu šādus pabalstus un pakalpojumus (MI akta III pielikumu 5. punkta a) apakšpunkts). Minētās sistēmas ir klasificētas kā augsta riska sistēmas, ņemot vērā, ka fiziskas personas, kuras piesakās pamata sociālās palīdzības pabalstiem un pakalpojumiem vai saņem tos no publiskām iestādēm, proti, veselības aprūpes pakalpojumus, sociālās nodrošināšanas pabalstus, sociālos pakalpojumus, kas nodrošina aizsardzību tādos gadījumos kā maternitāte, slimība, nelaimes gadījumi darbā, atrašanās apgādībā vai vecums un darba zaudēšana, kā arī sociālā palīdzība un palīdzība mājokļa jomā, parasti ir atkarīgas no minētajiem pabalstiem un pakalpojumiem un atrodas neaizsargātā pozīcijā attiecībā pret atbildīgajām iestādēm. Ja MI sistēmas lieto, lai noteiktu, vai iestādēm šādi pabalsti un pakalpojumi būtu jāpiešķir vai jāatsaka, jāsamazina, jāatsauc vai jāatgūst, tostarp, lai noteiktu, vai labuma guvējiem ir likumīgas tiesības uz šādiem pabalstiem vai pakalpojumiem, minētajām sistēmām var būt ievērojama ietekme uz personu iztiku, un tās var pārkāpt tādas personu pamattiesības kā tiesības uz sociālo aizsardzību, nediskriminēšanu, cilvēka cieņu vai efektīvu tiesību aizsardzību (MI akta 58. apsvērums).

Otrkārt, augsta riska sistēmas ir MI sistēmas, ko paredzēts izmantot fizisku personu kredītspējas izvērtēšanai vai to kredītnovērtējuma noteikšanai, izņemot tādas MI sistēmas, kuras izmanto krāpšanas atklāšanai finanšu jomā (MI akta III pielikumu 5. punkta b) apakšpunkts). Šīs MI sistēmas, ir klasificējamas kā augsta riska MI sistēmas, jo tās nosaka minēto personu piekļuvi

finanšu resursiem vai tādiem būtiskiem pakalpojumiem kā mājoklis, elektroenerģija un telesakaru pakalpojumi. Minētajiem nolūkiem lietotās MI sistēmas var izraisīt diskrimināciju starp personām vai grupām un var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, pamatojoties uz rasisko vai etnisko izcelsmi, dzimumu, invaliditāti, vecumu vai seksuālo orientāciju, vai var radīt jaunus diskriminējošas ietekmes veidus (MI akta 58. apsvērums).

Treškārt, augstu risku rada MI sistēmas, ko paredzēts izmantot riska novērtēšanai un cenu noteikšanai attiecībā uz fiziskām personām dzīvības un veselības apdrošināšanas gadījumā (MI akta III pielikumu 5. punkta c) apakšpunkts). Šīm MI sistēmām var būt ievērojama ietekme uz personu iztiku un, ja tās netiek pienācīgi projektētas, izstrādātas un lietotas, var pārkāpt viņu pamattiesības un radīt nopietnas sekas cilvēku dzīvībai un veselībai, tostarp finansiālu atstumtību un diskrimināciju (MI akta 58. apsvērums).

Ceturtkārt, augstu risku rada arī MI sistēmas, ko paredzēts izmantot, lai izvērtētu un klasificētu fizisku personu ārkārtas palīdzības izsaukumus vai ārkārtas pirmās reaģēšanas dienestu, tostarp policijas, ugunsdzēsēju un medicīniskās palīdzības sniedzēju, nosūtīšanai vai nosūtīšanas prioritāšu noteikšanai, kā arī neatliekamās medicīniskās aprūpes pacientu triāžas sistēmām (MI akta III pielikumu 5. punkta d) apakšpunkts). Minētās sistēmas ir klasificējamas kā augsta riska sistēmas, jo tās pieņem lēmumus personu veselībai un dzīvībai un to īpašumam izšķirīgi svarīgās situācijā (MI akta 58. apsvērums).

Turpmāk ir aplūkoti vairāki piemēri no starptautiskās prakses, kas parāda, kā MI sistēmu izmantošana var būt diskriminējoša un radīt būtisku kaitējumu personām.

Prakses piemēri

Sistēmas krāpšanas atklāšanai sociālās labklājības jomā

Nīderlandes lietā tika pierādīts, ka sistēmiskā riska identificēšanas (SyRI) krāpšanas apkarošanas sistēmas ieviešana, ko izmantoja, lai atklātu krāpšanu sociālās labklājības jomā, izraisīja diskrimināciju **ienākumu un etniskās izcelsmes dēļ.** No 2005. gada līdz 2019. gadam Nodokļu un

muitas administrācija (Belastingdienst) nepamatoti apsūdzēja aptuveni 26 000 vecāku par krāpnieciskiem pabalstu pieprasījumiem, pieprasot viņiem pilnībā atmaksāt saņemtos pabalstus. Tās izmantošana tika apturēta ar Hāgas tiesas sprieduma 2020. gadā.[73] 2021. gadā šis skandāls labklājības jomā piespieda Nīderlandes valdību atkāpties.

Mākslīgā intelekta sistēma atzīmēja vairāk nekā 20 000 vecāku kā krāpniekus saistībā ar bērna kopšanas pabalsta pieprasīšanu un Nīderlandes nodokļu iestādes veica izmeklēšanu. MI sistēma uzskatīja dubultpilsonību kā augsta riska faktoru un tā rezultātā tika uzsākti nesamērīgi daudz izmeklēšanas un tiesas procesi pret ģimenēm ar migrācijas izcelsmi, kurām tika apturēti bērna kopšanas pabalsti un daļai no tām tika lūgts atmaksāt saņemtos pabalstus.[74] Daudzos gadījumos summa sasniedza vairākus desmitus tūkstošu eiro, radot ģimenēm smagas finansiālās grūtības.[75]

Pat pēc Hāgas tiesas 2020. gada pašvaldības iestādes visā Nīderlandē turpināja izmantot algoritmus, lai atklātu krāpšanas riskus. Šīs sistēmas un lietojumprogrammas atšķiras pēc sarežģītības, taču daudzos gadījumos tām var būt liela ietekme. Daudzas no šīm sistēmām izmanto algoritmus, lai, pamatojoties uz vēsturiskajiem datiem, novērtētu atsevišķu saņēmēju vai noteiktu saņēmēju grupu krāpšanas iespējamību. Lai identificētu personas vai grupas kā potenciālos krāpniekus, tiek izmantota pagātnes pieredze, riska uztvere, kā arī rādītāji, kuriem nav zināma izcelsme vai vērtība. Piemēram, tāda profesija kā frizieris var radīt lielāku krāpšanas risku nekā advokāta profesija. Iespējams, ka cilvēkiem, kam pieder savas mājas, var būt daudz mazāka iespēja tikt atzīmētiem kā potenciāliem krāpniekiem, nekā cilvēkiem, kas dzīvo īrētās mājās.[76]

Roterdamā 2021. gadā pēc Roterdamas Revīzijas palātas veiktās izmeklēšanas par algoritmu izstrādi un izmantošanu pilsētā tika pieņemts lēmums apturēta labklājības algoritma izmantošana. Valdības revidents konstatēja, ka starp algoritmu izstrādātājiem un pilsētas darbiniekiem, kas tos izmanto, ir "nepietiekama koordinācija", kas var novest pie ētisku apsvērumu neievērošanas. Ziņojumā arī tika kritizēta pilsēta par to, ka tā nav novērtējusi, vai algoritmi ir labāki par sistēmām,

[73] Vervloesem, K. (6 April, 2020). How Dutch activists got an invasive fraud detection algorithm banned, *AlgorithmWatch*; Heikkilä, M. (29 March, 2022). Dutch scandal serves as a warning for Europe over risks of using algorithms. *Politico*; Henley, J. (14 January, 2021). Dutch government faces collapse over child benefits scandal. *The Guardian*.

[74] Sk. ten Seldam, B, Brenninkmeijer, A. (30 April, 2021). The Dutch benefits scandal: a cautionary tale for algorithmic enforcement. *EU Law Enforcement*.

[75] H Heikkilä, M. (29 March, 2022). Dutch scandal serves as a warning for Europe over risks of using algorithms. *Politico*.

[76] Dutch Data Protection Authority. (2023). Algorithmic Risks Report Netherlands.

kas balstās uz cilvēku izvērtējumu, kuras tie aizstāj. Izceļot labklājības krāpšanas algoritmu, ziņojumā konstatēts, ka pastāv neobjektīvu rezultātu iespējamība, pamatojoties uz datu veidiem, kas izmantoti personu riska rādītāju noteikšanai.[77]

Šo sistēmu izmantošana, kas novērtē indivīda iespējamo krāpšanas risku, var ietekmēt indivīdu, ģimeņu un sabiedrības grupu dzīvi. Tikt atzīmētam kā potenciālam krāpnieks var radīt cilvēkiem ievērojamu emocionālu un finansiālu kaitējumu. Cilvēki jau no paša sākuma tiek turēti aizdomās, un izmantoto sistēmu necaurredzamības dēļ viņiem ir grūti noskaidrot, kāpēc viņi tiek klasificēti kā krāpnieki un ko viņi var darīt lietas labā. Mērogs, kādā tas notiek, var arī pārvērst šo individuālo kaitējumu būtiskā kaitējumā sabiedrībai, ko skaidri parāda strīdi par sociālajiem pabalstiem un SyRI sistēmu.[78]

Līdzīgas problēmas saistībā ar algoritmu risku nepienācīgu pārvaldīšanu ir atklātas arī citās valstīs. Spilgts piemērs ir **"Robodebt skandāls" Austrālijā**, kas parāda, kādas var būt sekas automatizētas lēmumu pieņemšanai bez cilvēka uzraudzības un bez "drošības tīkla" modeļa kļūdu atklāšanai.[79] Šajā gadījumā nekontrolēta algoritmisku lēmumu pieņemšana radīja būtisku ietekmi uz cilvēku dzīvi. Robodebt skandāla lietā ienākumu skaitļi no gada nodokļu deklarācijām cilvēkiem, kas saņēma pabalstus, tika salīdzināti ar ienākumu deklarāciju, kas tiek sniegta reizi divās nedēļās aģentūrā, un process tika pilnībā automatizēts. Ja skaitļi no abām datu plūsmām nesakrita, algoritms aprēķināja, ka kāds ir saņēmis pārāk lielu pabalstu un ka viņam būs tas jāatmaksā. Pēc tam pilnīgi automatizēti bez amatpersonas apstiprināšanas parādniekam tika nosūtīta vēstule ar atmaksājamo summu. Taču modelī netika ņemtas vērā ienākumu svārstības, piemēram, sezonas darbiniekiem. Tādējādi **iedzīvotāju grupām ar mainīgiem ienākumiem** tika kļūdaini uzlikti milzīgi naudas sodi. Šie sodi ir radījuši lielas personiskas problēmas personām, kas ļoti ietekmējuši šo iedzīvotāju grupu un viņu ģimenes.

Līdzīgi arī **Apvienotajā Karalistē** Darba un pensiju departaments izmantotais krāpšanas apkarošanas algoritms liecina par atbilstošas kontroles nozīmi, lai nodrošinātu taisnīgumu.[80] Darba un pensiju departaments izmantoja algoritmus, lai cīnītos pret krāpšanu ar pabalstiem. Tajā pašā laika posmā lielai daļai Apvienotajā Karalistē dzīvojošo **bulgāru sieviešu pabalst**i tika pārtraukti. Tas obligāti nenozīmē, ka pastāvēja diskriminācija, bet problēma ir tā, ka pats Darba un pensiju

[77] Burgess, M. (6 March, 2023). This Algorithm Could Ruin Your Life. *Wired*.
[78] Dutch Data Protection Authority. (2023). Algorithmic Risks Report Netherlands.
[79] Dutch Data Protection Authority. (2024). AI & Algorithmic Risks Report Netherlands. Report winter 2023/2024.
[80] Turpat.

departaments to nevarēja droši pateikt. Tas norādīja, ka algoritmu negodīgu rezultātu pārbaužu rezultāti nav skaidri. Tas liecina par atbilstošu kontroles pasākumu trūkumu un līdz ar to atbildīgas algoritma izmantošanas nenodrošināšanu.

Atbildības un pārredzamības trūkums pār MI sistēmu izmantošanu var novest pie tā, ka personas, attiecībā uz kurām MI sistēmas pieņem lēmumus, nevar sniegt paskaidrojumus vai pārsūdzēt lēmumus. Pārredzamība ir viena no būtiskām prasībām, kas jānodrošina, izmantojot MI sistēmas, kas noteikta arī MI aktā.

Krāpšanas prognozēšanas algoritmi rada augstu risku, un tāpēc to izmantošanai ir vajadzīgas atbilstošas pārbaudes un līdzsvara procedūras (angļu val. - checks and balances). Jāizveido iestādes, kas nepārtraukti uzraudzītu un identificētu šāda algoritma izmantošanas riskus. Pārbaudēm jāattiecas gan uz šādu sistēmu izstrādi, gan ieviešanu, jo riski var rasties un tikt pamanīti abos posmos. Gan krāpšanas prognozēšanas sistēmu izstrādes, gan ieviešanas posmā ir jānovērtē algoritma lietderība attiecībā pret riskiem pamattiesībām un sabiedrības vērtībām. Sistēmas, kas paredz krāpšanu, rada augstu risku sabiedrības vērtībām un pamattiesībām. Tāpēc tās ir pastāvīgi jānovērtē. Vajadzības gadījumā jāveic atbilstoši pasākumi. Dažkārt atteikšanās no šo augsta riska sistēmu izmantošanas var būt viens no lēmumiem, ja izrādās, ka ieguvumi nepietiekami atsver riskus sabiedrības vērtībām un pamattiesībām. [81]

Sejas atpazīšanas tehnoloģiju izmantošana, lai piekļūtu sabiedriskiem pakalpojumiem

Sejas atpazīšanas tehnoloģiju izmantošana sabiedriskajos pakalpojumos vai saistībā ar tiem var novest pie sabiedrisku pakalpojumu liegšanas gala lietotājiem. Piemēram, Vācijā Hamburgā Valsts transporta biroja fotokabīne neatpazina pieteikuma iesniedzējas seju, lai uzņemtu biometrisko attēlu, kas bija nepieciešams viņas administratīvā pieteikuma iesniegšanai. Lai gan Valsts transporta birojs noliedza, ka kļūda būtu radusies izmantotās sejas atpazīšanas programmatūras dēļ, biroja darbinieks norādīja, ka kļūdas bieži notiek saistībā ar pieteikuma iesniedzēja **ādas krāsu**.[82]

Aizdevuma atteikums kredītiestādē

[81] Dutch Data Protection Authority. (2023). Algorithmic Risks Report Netherlands.
[82] Sk. Bartoletti, I., Xenidis, R. (2023). Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Council of Europe; Wulf, J. (2022). Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected, *AlgorithmWatch*.

Vācijā sievietei kredītiestāde atteica kredītu, iegādājoties preces tiešsaistē. Izmeklējot kredītiestādes atteikuma iemeslus, kliente uzzināja, ka viņas **vecuma** un **dzimuma** kombinācija, šķiet, ir motivējusi automatizēto atteikumu, balstoties uz netaisnīgiem stereotipiem, ka sievietes ap 40 gadiem bieži ir šķīrušās un tāpēc viņām ir mazāki naudas līdzekļi.[83]

Somijā Valsts nediskriminācijas un vienlīdzības tribunāls konstatēja tiešu daudzkārtēju diskrimināciju lietā, kurā pieteikuma iesniedzējam tika atteikts aizdevums tiešsaistē. Pēc lietas izmeklēšanas Līdztiesības iestāde (Nediskriminācijas ombuds) konstatēja, ka uzņēmums ir izmantojis statistikas modeļus, lai novērtētu kredītspēju, kas balstījās uz pieteikuma iesniedzēja **vecumu, dzimumu, valodu un dzīvesvietu**, vienlaikus neņemot vērā pieteikuma iesniedzēja faktisko kredītvēstures stāvokli. Konkrētajā gadījumā pieteikuma iesniedzējs, kurš bija vīrietis, runāja somu valodā un bija no laukiem, finanšu iestādes veiktajā novērtējumā tika uzskatīts par nelabvēlīgu faktoru.[84]

Kredītlimita noteikšana

ASV Ņujorkas Finanšu pakalpojumu departaments izmeklēja iespējamo diskrimināciju dzimuma dēļ saistībā ar kredītlimita piešķiršanu.[85] Tā tika veikta pēc tam, kad 2019. gadā tehnoloģiju uzņēmējs Deivids Heinemeiers Hansons (David Heinemeier Hansson) Twitter publicēja ziņas, ka viņam tika piedāvāts Apple kredītkartes kredītlimits 20 reizes lielāks nekā viņa sievai, lai gan abi iesniedza kopīgas nodokļu deklarācijas un viņai bija labāks kredītreitings. Virknē tvītu viņš norādīja, kredītlimita atšķirības ir saistītas ar diskrimināciju **dzimuma dēļ**. Viņš arī pauda bažas, ka lēmums par kredītu tika pieņemts, izmantojot algoritmus un mašīnmācīšanos, un ka Apple Card klientu apkalpošanas aģents nevarēja izskaidrot šos algoritmus vai kredītlimitu atšķirības pamatojumu. Apple un Goldman Sachs izlaida Apple Card 2019. gada augustā. Goldman Sachs bija atbildīgs par Apple Card kredītpolitiku un parakstīšanas lēmumiem, kā arī par Apple kartes pārvaldību. Atbildot uz sūdzībām, Goldman Sachs banka norādīja, ka tā nav ņēmusi vērā dzimumu, nosakot kredītspēju un noraidīja apsūdzības par diskriminēšanu dzimuma dēļ. Ņujorkas Finanšu pakalpojumu departaments 2021. gadā pieņēma lēmumu, kurā tas nekonstatēja pierādījumus par prettiesisku

[83] Sk. Wulf, J. (2022). Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected, *AlgorithmWatch*.
[84] Bartoletti, I., Xenidis, R. (2023). Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Council of Europe; Sk. Matzat, L. (21 Novembre, 2018). Finnish Credit Score Ruling raises Questions about Discrimination and how to avoid it. *AlgorithmWatch*; Hiltunen, R. (1 August, 2018). Multiple discrimination in assessing creditworthiness. *European network of legal experts in gender equality and non-discrimination*.
[85] New York State Department of Financial Services. (2021). *Report on Apple Card Investigation*.

diskrimināciju pārkāpumu. Vienlaikus, tas uzsvēra nepieciešamību veicināt inovācijas, kas uzlabo piekļuvi kredītiem, vienlaikus saglabājot stingrus standartus, lai novērstu diskrimināciju. Minētā lieta vērsa plašu sabiedrības uzmanību uz diskriminācijas risku kredīta piešķiršanas jomā.[86]

Konta atvēršana tiešsaistē

AlgorithmWatch pētījums atklāja, ka digitālā diskriminācija sniedzas daudz tālāk par mākslīgo intelektu.[87] Vienkāršas tiešsaistes veidlapas var izraisīt **diskrimināciju rases, etniskās izcelsmes vai tautības dēļ**, piemēram, ja tās ļauj reģistrēt tikai ar vārdiem, kuros ir trīs vai vairāk burti. Pretendentiem ar īsākiem vārdiem tiks liegta reģistrācija vai viņi nevarēs atvērt kontu, kas bieži vien ir priekšnoteikums preču un pakalpojumu iegādei tiešsaistē.

Diskriminējoša apdrošināšanas polises cenas

Itālijas Padujas, Udīnes, Kārnegija un Melona universitāšu veiktais pētījums apdrošināšanas nozarē parādīja, ka tādi faktori kā **dzimšanas vieta un pilsonība** ietekmē **automašīnu apdrošināšanas polišu cenu**, ko maksā klienti.[88] Gadījuma izpētē viņi parādīja, ka Gana kā pieteikuma iesniedzēja dzimšanas vieta varētu izraisīt cenu pieaugumu par 1000 EUR, salīdzinot ar pieteikuma iesniedzēju, kurš kā savu dzimteni norāda Itāliju.

Līdzīgs arī ProPublica izmeklēšanā ASV tika atklāts, ka cilvēki **mazākumtautību rajonos** vidēji maksāja lielākas automašīnu apdrošināšanas prēmijas nekā iedzīvotāji, kas dzīvoja rajonos, kuros pamatā dzīvo baltādainie, neskatoties uz līdzīgām negadījumu izmaksām. Lai gan žurnālisti nevarēja apstiprināt šo atšķirību cēloni, viņi norāda, ka vainīgi varētu būt neobjektīvi algoritmi.[89]

---

[86] Sk. Vigdor, N. (10 November, 2019). Apple Card Investigated After Gender Discrimination Complaints. *The New York Times*; Knight W. (19 November, 2019). The Apple Card Didn't 'See' Gender—and That's the Problem. *Wired*.
[87] AlgorithmWatch. (13 January 2022). Fixing Online Forms Shouldn't Wait Until Retirement.
[88] Bartoletti, I., Xenidis, R. (2023). Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Council of Europe; Sk. Wulf, J. (2022). Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected, *AlgorithmWatch*.
[89] Centre for Data Ethics and Innovation. (2020). Review into bias in algorithmic decision-making; Angwin, J., Larson, J., Kirchner, L. et al. (5 April, 2017). Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk. ProPublica.

Studentu kredītu piešķiršanas pārbaude

Nīderlandes aģentūra – Studentu finanšu dienests (Dienst Uitvoering Onderwijs), kas ir atbildīga par studentu kredītu piešķiršanu un samaksu tiem, kas iestājušies Nīderlandes augstākajā izglītībā - izmantoja algoritmu, lai pārbaudītu, vai studentu kredīti ir piešķirti pareizi un vai nenotiek krāpšana. 2012. gadā tā sāka izmantot algoritmu, kas "netieši diskriminēja" **jauniešus ar etnisko minoritāšu izcelsmi**. Šie studenti tika "ievērojami biežāk" apsūdzēti studiju kredītu vai stipendiju izkrāpšanā nekā citi studenti. Izglītības ministrs, kura pārziņā ir aģentūra, apturēja algoritma izmantošanu 2023. gadā.[90]

No 376 lietām, kurās bija iesaistīti juristi, 97% bija studenti ar mazākumtautību izcelsmi. Studentiem, kuri dzīvo ārpus mājām, ir tiesības uz lielāku stipendiju, un no 2012. līdz 2023. gadam gandrīz 27 000 studentu apmeklēja amatpersonas, lai pārbaudītu viņu dzīvesvietu. Gandrīz 10 000 no viņiem faktiski tika apsūdzēti krāpšanā. Kopš 2012. gada Studentu finanšu dienests ir izmantojis algoritmu, lai meklētu iespējamo krāpšanu, pamatojoties uz tādiem iespējamiem riska rādītājiem kā vecums un izglītība, un apmācīts, izmantojot izmeklētāju "pieredzi". Kad aizdomās turamais ir identificēts, krāpšanas izmeklētāji izlemj, vai viņu vajadzētu pārbaudīt. Piemēram, jaunieši, kuri dzīvo kopā ar ģimenes locekļiem, piemēram, brāli vai tanti, rada potenciālu risku, lai gan viņiem saskaņā ar likumu ir tiesības saņemt stipendiju par aptuveni 200 eiro mēnesī vairāk nekā mājās dzīvojošajam studentiem. Studentu finanšu dienesta izmantotā sistēma netieši novedusi pie tā, ka skolēni ar etnisko minoritāšu saknēm saskaras ar diskrimināciju – nevis viņu izcelsmes, bet gan citu kontrolsarakstā ietverto kritēriju dēļ.[91]

Daudzie prakses piemēri, jo īpaši Nīderlandē, parāda gan ieguvumus, gan nepilnības saistībā ar automatizētās lēmumu pieņemšanas turpmāku integrēšanu valsts pārvaldē. No vienas puses, tas var samazināt izmaksas un palielināt efektivitāti. No otras puses, automatizētu lēmumu pieņemšanas sistēmās var būt kļūdainas un nespēt ievērot sarežģītus sociālos un juridiskos aspektus.[92]

Aplūkotie piemēri liecina, ka gan valsts iestādes, kas piešķir un aprēķina pabalstus un sniedz sabiedriskus pamatpakalpjumus, gan kredītiestādes un apdrošināšanas uzņēmumi, kas piešķir

[90] DutchNews. (1 March, 2024). "Student finance group Duo did discriminate in fraud probes".
[91] Turpat; NL Times. (22 MAY 2024). Education agency discriminated against even more ethnically diverse students: new study.
[92] De Heer, S. (25 July, 2023). A Scandal on AI in Administration, Again. *Verfassungsblog*.

kredītus un dzīvības un veselības apdrošināšanu, var izmantojot algoritmus un MI sistēmas, kas darbojas kļūdaini un neobjektīvi, un balstoties uz tām pieņemt nepamatotus un diskriminējošus lēmumus.

8. Kopsavilkums

Neraugoties uz plašo **ES diskriminācijas aizlieguma tiesiskā regulējuma** darbības jomu, regulējumam, kas paredz aizsardzību pret diskrimināciju dzimuma un rases dēļ, ir daudzas nepilnības, kas ir problemātiskas algoritmiskās diskriminācijas kontekstā. Šī situācija ir vēl problemātiskāka attiecībā uz citiem aizsargātiem pamatiem — vecumu, invaliditāti, seksuālo orientāciju un reliģiju —, kuriem saskaņā ar ES tiesību aktiem ir ierobežota aizsardzība. Algoritmiskā diskriminācija rada izaicinājumus robežu noteikšanai starp tiešu un netiešu diskrimināciju, mazinot juridisko noteiktību. Latvijā diskriminācijas aizliegums ir konstitucionāli nostiprinātas pamattiesības, kā arī to paredz daudzi citi Latvijas tiesību akti. Tajā pašā laikā diskriminācijas aizlieguma regulējums nav pietiekams, lai efektīvi aizsargātu pret algoritmisko un MI sistēmu radīto diskriminācijas risku.

Lai novērstu algoritmu vai MI sistēmu izmantošanas rezultātā radītos diskriminācijas riskus, būtiska nozīme ir **datu aizsardzības regulējumam**. Datu aizsardzības principi ir piemērojami arī MI sistēmām, kas apstrādā personas datus. Piemēram, godprātības princips paredz automatizētu lēmumu satura godprātīgumu jeb taisnīgumu. VDAR 22. pants nosaka personu tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz personu rada tiesiskās sekas vai kas līdzīgā veidā to ievērojami ietekmē. Vienlaikus ir paredzēti izņēmumi no šī aizlieguma, kā arī aizsardzības garantijas. Aizsardzības pasākumi automatizētu lēmumu pieņemšanas gadījumā cita starpā ietver tiesības panākt cilvēka līdzdalību; tiesības būt informētam par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana; tiesības saņemt jēgpilnu informāciju par automatizētajā lēmumā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām. Informēšanas pienākums ir saistīts ar fundementālu un problemātisku jautājumu par MI sistēmu un to rezultātu, kā arī ar to saistīto cilvēka pieņemto lēmumu izskaidrojamību, ko cenšas risināt ES MI regulējums.

MI akta viens no galvenajiem mērķiem ir novērst MI sistēmu radītos riskus pamattiesībām, tai skaitā diskriminācijas riskus. MI akts nesamazina aizsardzību, tostarp prakses aizliegumus, ko nosaka diskriminācijas novēršanas un datu aizsardzības tiesiskais regulējums, bet gan papildina esošo regulējumu. MI aktā ir izmantota uz risku balstīta pieeja, klasificējot MI sistēmas atkarībā no dažādiem to radītajiem riska līmeņiem. Tas aizliedz vairākus nepieņemamus MI prakses veidus, kas ir pretrunā ES vērtībām un pamattiesībām, nosaka prasības augsta riska MI sistēmām,

pārredzamības pienākumus attiecībā uz dažām MI sistēmām, kā arī saskaņotus noteikumus par vispārīga lietojuma MI modeļu laišanu tirgū. MI akts paredz divu veidu augsta riska sistēmas: sistēmas, kuras ir produktu vai sistēmu drošības sastāvdaļas vai pašas ir produkti vai sistēmas, uz ko attiecas daži ES saskaņošanas tiesību akti, kas uzskaitīti I pielikumā; III pielikumā minētās MI sistemas. MI akta III pielikumā uzskaitītas astoņas jomas, kurās MI izmantošana rada augstu risku. Tajā pašā laikā MI akts paredz, ka minētās MI sistēmas neuzskata par augsta riska sistēmām, ja tās nerada būtisku kaitējuma risku fizisku personu veselībai, drošībai vai pamattiesībām, tostarp būtiski neietekmē lēmumu pieņemšanas iznākumu. Šī papildus kritērija piemērošana praksē ir efektīvi jāuzrauga, lai nodrošonātu, ka augsta riska MI sistēmas tiek atbilstoši klasificētas. Augsta riska sistēmām ir noteiktas daudzas obligātas prasības saistībā ar riska pārvaldību, tehnisko dokumentāciju un uzskaiti, pārredzamību un informācijas sniegšanu uzturētājiem, cilvēka virsvadību un robustumu, precizitāti un kiberdrošību, kā arī izmantoto datu kopu kvalitāti un nozīmīgumu. Augstas kvalitātes datiem ir īpaši svarīga nozīme, lai novērstu MI sistēmu izmanošanas radītos diskriminācijas riskus. Pētījumā palūkotie prakses piemēri parāda, ka visās četrās pētījumā analizētajās augsta riska jomās MI sistēmas var radīt diskriminācijas riskus.

Biometrijas jomā augstu risku rada trīs veidu MI sistēmas: biometriskās tālidentifikācijas sistēmas; MI sistēmas, ko paredzēts izmantot biometriskai kategorizēšanai pēc sensitīviem vai aizsargātiem atribūtiem vai raksturlielumiem; MI sistēmas, ko paredzēts izmantot emociju atpazīšanai (MI akta III pielikuma 1. punkts). Minētās sistēmas ir uzskatāmas par augsta riska sistēmām, ja vien tās nav klasificējamas kā aizliegtas MI sistēmas saskaņā ar ES vai valstu tiesību aktiem. Saskaņā ar MI aktu visas šīs sistēmas var tikt arī klasificētas kā aizliegtas MI sistēmas. Proti, MI akts aizliedz reāllaika biometriskās tālidentifikācijas izmantošanu sabiedriskās vietās tiesībaizsardzības nolūkos; biometriskās kategorizācijas sistēmas, kas ļauj noteikt vai izsecināt personas rasi, politiskos uzskatus, dalību arodbiedrībās, reliģiskos vai filozofiskos uzskatus, dzimumdzīvi vai seksuālo orientāciju; kā arī emociju atpazīšanu darbavietā un izglītības iestādēs. Viens no izaicinājumiem, ir MI sistēmu pareiza klasificēšana, ņemot vērā, ka arī tāda prakse, kas nav klasificēta kā aizliegta prakse saskaņā ar MI aktu, var būt aizliegta saskaņā ar citiem ES vai dalībvalstu tiesību aktiem.

Pastāv daudzi prakses piemēri, īpaši ASV un Apvienotajā Karalistē, kas parāda, ka sejas atpazīšanas tehnoloģiju izmantošana policijas darbā rada diskriminācijas risku un var būt neobjektīvas, īpaši rases un dzimuma dēļ. MI sistēmu rezultātus būtiski ietekmē algoritmu vai programmatūras izstrādē izmantoto datu kvalitāte, kas var atspoguļot neobjektivitāti, neprecizitātes un kļūdas datu vākšanas procesā. Neprecizitāti izraisa pārstāvība datu kopās, ko izmanto, lai izveidotu un

apmācītu algoritmus. Datu kvalitātei nepieciešams liels daudzums sejas attēlu, kas ietver dažādas cilvēku grupas. Tomēr daudzos gadījumos algoritmu izveidei tiek vairāk izmantoti baltādaino vīriešu sejas attēli, mazāk – sieviešu un citas etniskās izcelsmes personu attēli. Tāpēc sejas atpazīšanas sistēmas labi darbojas attiecībā uz baltādainiem vīriešiem, bet ievērojami sliktāk tās atpazīst melnādainos vīriešus un sievietes. Viena no galvenajām problēmām ir pārredzamības trūkums. Trūkst arī skaidrs un efektīvs kompensācijas mehānisms personām un kopienām, kurām ir nodarīts kaitējums policijas izmantoto sejas atpazīšanas tehnoloģiju dēļ.

Izglītības un arodapmācības jomā par augsta riska sistēmām uzskata MI sistēmas, ko izmanto šādos četros veidos: lai noteiktu piekļuvi izglītībai, iestāšanos vai uzņemšanu izglītības iestādē; lai izvērtētu mācību rezultātus; lai novērtētu izglītības līmeni, ko persona varēs saņemt; kā arī lai pārbaudījumu laikā izglītības un arodmācības iestādēs uzraudzītu un konstatētu audzēkņu neatļautu uzvedību (MI akta III pielikuma 3. punkts).

Aplūkotie prakses piemēri izglītības jomā liecina, ka diskriminācijas risku rada dažāda veida MI sistēmas: tiešsaistes eksāmenu uzraudzības programmatūra; programmas MI radīta teksta noteikšanai; algoritmu izmantošana eksāmenu vērtēšanā; MI sistēmu izmantošana uzņemšanai augstskolās. Viena no būtiskām problēmām ir iespējama neobjektivitāte MI algoritmos, ko izmanto studentu profilēšanai. Algoritmi var atspoguļot izglītības sistēmā esošus aizspriedumus, piemēram, rases vai dzimuma dēļ. Piemēram, ja mākslīgā intelekta sistēma, kas tiek izmantota studentu vērtēšanā, ir apmācīta uz vēsturiskiem datiem, kas atspoguļo aizspriedumus, tā var negodīgi nostādīt neizdevīgākā situācijā noteiktas studentu grupas. MI sistēmas, kas iesaka kursus vai karjeras izvēli, var būt neobjektīvas attiecībā uz noteiktām demogrāfiskajām grupām, ja apmācību datos ir ietverti sabiedrības aizspriedumi un stereotipi, radot nevienlīdzību.

Personas ir jāinformē, ka tās saskaras ar MI sistēmu vai algoritmiem, lai tās varētu apstrīdēt rezultātu un šādu sistēmu izmantošanu. Apskatītie prakses gadījumu liecina, ka MI sistēmu un algoritmu iespējamās negatīvās sekas ne vienmēr ir viegli izvērtējamas. Izglītības iestādēm būtu jānodrošina, ka studenti ir informēti par to, kā tiek izmantoti viņu dati, un ka viņiem ir iespēja atteikties no profilēšanas, izmantojot MI sistēmas. MI algoritmi ir regulāri jāpārbauda, kā arī ir jāveic atbilstoši pasākumi, lai novērstu neobjektīvus rezultātus un diskriminējošas sekas.

Nodarbinātības, darba ņēmēju pārvaldības un piekļuves pašnodarbinātībai jomā augstu risku rada MI sistēmas, ko paredzēts izmantot divos veidos: fizisku personu pieņemšanai darbā vai darbinieku atlasei; lai pieņemtu lēmumus, kas skar darba attiecību, paaugstināšanas amatā vai

darba līgumattiecību izbeigšanas kārtību, sadalītu uzdevumus, pamatojoties uz individuālo uzvedību vai personības iezīmēm vai īpašībām, vai lai pārraudzītu un izvērtētu darba līgumattiecībās esošo personu sniegumu un uzvedību (MI akta III pielikuma 4. punkts).

Pētījumā aplūkotie prakses gadījumi liecina, ka nodarbinātības jomā MI sistēmu izmantošana var radīt diskrimināciju, īpaši dzimuma dēļ. 2021. gadā Amazon atteicās no MI personāla atlases rīka, kas bija diskriminējošs pret sievietēm. Nīderlandē tika konstatēts, ka darba meklēšanas platformā valodas lietojums atkarībā no dzimuma, meklējot sludinājumus, sniedz atšķirīgus rezultātus par darba iespējām. Arī darba sludinājumu izplatīšana, izmantojot sociālo mediju platformu piedāvātos pakalpojumus, var veicināt dzimumu stereotipus. Minētās sistēmas var nostiprināt vēsturiskos diskriminācijas modeļus, piemēram, attiecībā uz sievietēm, dažām vecuma grupām, personām ar invaliditāti vai personām ar noteiktu etnisko vai rases piederību vai seksuālo orientāciju.

Piekļuves pamatpakalpojumiem un sabiedriskajiem pakalpojumiem un pabalstiem jomā augstu risku rada MI sistēmas, ko paredzēts izmantot četros veidot: publiskajās iestādēs, lai izvērtētu personu tiesības saņemt sociālās palīdzības pabalstus un pakalpojumus; personu kredītspējas izvērtēšanai vai to kredītnovērtējuma noteikšanai; riska novērtēšanai un cenu noteikšanai dzīvības un veselības apdrošināšanas gadījumā; lai izvērtētu un klasificētu personu ārkārtas palīdzības izsaukumus vai ārkārtas pirmās reaģēšanas dienestu nosūtīšanai (MI akta III pielikuma 5. punkts).

Pētījumā aplūkotie prakses piemēri liecina, ka gan valsts iestādes, kas piešķir un aprēķina pabalstus un sniedz sabiedriskus pamatpakalpojumus, gan kredītiestādes un apdrošināšanas uzņēmumi, kas piešķir kredītus un dzīvības un veselības apdrošināšanu, var izmanotot algoritmus un MI sistēmas, kas darbojas kļūdaini un neobjektīvi, un balstoties uz tām pieņemt nepamatotus un diskriminējošus lēmumus.

Prakses piemēri Nīderlandē, Apvienotajā Karalistē, kā arī Austrālijā atklāj, ka sistēmas krāpšanas atklāšanai sociālās labklājības jomā var radīt diskrimināciju, lielākoties ienākumu jeb sociālā stāvokļa un etniskās izcelsmes dēļ. Atbildības un pārredzamības trūkums pār MI sistēmu izmantošanu var novest pie tā, ka personas, attiecībā uz kurām MI sistēmas pieņem lēmumus, nevar sniegt paskaidrojumus vai pārsūdzēt lēmumus. Krāpšanas prognozēšanas algoritmi rada augstu risku, tāpēc to izmantošanai ir vajadzīgas samērīguma pārbaudes gan izstrādes, gan ieviešanas posmā. Abos posmos ir jānovērtē algoritma lietderība attiecībā pret riskiem pamattiesībām un sabiedrības vērtībām. Ja tiek konstatēts, ka ieguvumi nepietiekami atsver riskus

sabiedrības vērtībām un pamattiesībām, viens no iznākumiem var būt arī atteikšanās no augsta riska sistēmu izmantošanas.

Prakses piemēri atklāj, ka arī MI sistēmas, ko izmanto personas kredītspējas izvērtēšanā, kā arī cenu noteikšanai apdrošināšanas gadījumā var būt diskriminējošas. Vācijā un Somijā personām tika atteikts aizdevums tiešsaistē vecuma, dzimuma, valodas un dzīvesvietas dēļ. Itālijā veiktais pētījums apdrošināšanas nozarē parāda, ka tādi faktori kā dzimšanas vieta un pilsonība var ietekmēt automašīnu apdrošināšanas polišu cenu, ko maksā klienti.

Rekomendācijas

Prakses piemēri atklāj vairākus kopīgus vispārējus izaicinājumus, ko MI sistēmas rada diskriminācijas aizlieguma principam un attiecīgas prasības, kas jāievēro, lai mazinātu un novērstu diskriminācijas riskus:

- **Datu kvalitāte un datu pārvaldība.** Lai novērstu MI sistēmu radītos diskriminācijas riskus, būtiska nozīme ir MI aktā ietvertajām prasībām nodrošināt augstu datu kvalitāti un atbilstošu datu pārvaldību. Algoritmu un to izvaddatu kvalitāte, precizitāte, derīgums un uzticamība lielā mērā ir atkarīga no ievaddatu kvalitātes, precizitātes, derīguma un uzticamības. Ja MI sistēma nav apmācīta ar augstas kvalitātes datiem, neatbilst attiecīgām veiktspējas, precizitātes vai robustuma prasībām vai nav pienācīgi projektēta un testēta pirms laišanas tirgū vai citādas nodošanas ekspluatācijā, tā var sniegt diskriminējošu iznākumu. Saskaņā ar MI aktu apmācības, validēšanas un testēšanas datu kopām ir jābūt atbilstošām, pietiekami reprezentatīvām un, cik vien iespējams, bez kļūdām un pilnīgām, ņemot vērā MI sistēmas paredzēto nolūku. Datu kopām ir jābūt atbilstošiem statistiskajiem raksturlielumiem, tostarp attiecībā uz personām vai personu grupām, attiecībā uz kurām ir paredzēts lietot augsta riska MI sistēmu. Īpaša uzmanība cita starpā ir jāpievērš tādas iespējamās neobjektivitātes mazināšanai datu kopās, kura varētu ietekmēt cilvēku veselību un drošību, nelabvēlīgi ietekmēt pamattiesības vai izraisīt diskrimināciju, jo īpaši, ja izvaddati ietekmē ievaddatus turpmākām darbībām (atgriezeniskās saites cilpas). Augsta riska MI sistēmas, kas turpina mācīties pēc to laišanas tirgū vai nodošanas ekspluatācijā, jāizstrādā tā, lai, cik vien iespējams, likvidētu vai samazinātu šādu iespējamu neobjektīvu iznākumu risku, kas ietekmē ievaddatus nākamās operācijās.

- **Pārredzamība un izskaidrojamība.** Pārredzamība ir viena no būtiskām prasībām, kas jānodrošina, izmantojot MI sistēmas, kas noteikta MI aktā. Pārredzamība nozīmē, ka MI sistēmas tiek projektētas un lietotas tā, lai būtu iespējama pienācīga izsekojamība un izskaidrojamība un vienlaikus lai cilvēki apzinātos, ka sazinās vai ir saskarē ar MI sistēmu, kā arī lai pienācīgi informētu uzturētājus par MI sistēmas spējām un ierobežojumiem un skartās personas – par to tiesībām. Lai kliedētu bažas, kas saistītas ar dažu MI sistēmu nepārredzamību un sarežģītību, pirms augsta riska MI sistēmu laišanas tirgū vai nodošanas ekspluatācijā ir jānodrošina to pārredzamība. Augsta riska MI sistēmas jāprojektē tā, lai uzturētāji varētu saprast, kā MI sistēma darbojas, izvērtēt tās funkcionalitāti un izprast tās stiprās puses un ierobežojumus. Augsta riska MI sistēmām būtu jāpievieno atbilstoša informācija, kas ietverta lietošanas instrukcijā. Šādai informācijai būtu jāietver MI sistēmas raksturlielumi, spējas un veiktspējas ierobežojumi, tai skaitā par iespējamiem zināmiem un paredzamiem apstākļiem, kuri saistīti ar augsta riska MI sistēmas lietošanu, tostarp uzturētāja darbību, kas var ietekmēt sistēmas uzvedību un veiktspēju, un kuros MI sistēma var radīt riskus veselībai, drošībai un pamattiesībām, kā arī par attiecīgajiem cilvēka virsvadības pasākumiem.

- **Cilvēka virsvadība.** Cilvēka virsvadība nozīmē, ka MI sistēmas tiek projektētas un lietotas kā instruments, kas kalpo cilvēkiem, respektē cilvēka cieņu un personisko autonomiju un darbojas tādā veidā, ko cilvēki var pienācīgi kontrolēt un virsvadīt. Saskaņā ar MI aktu augsta riska MI sistēmas jāprojektē un jāizstrādā tā, lai fiziskas personas varētu virsvadīt to funkcionēšanu, nodrošināt, ka tās tiek lietotas, kā paredzēts, un ka to ietekmei tiek pievērsta uzmanība visā sistēmas darbmūžā. Šajā nolūkā sistēmas nodrošinātājam pirms sistēmas laišanas tirgū vai nodošanas ekspluatācijā būtu jānosaka piemēroti cilvēka virsvadības pasākumi. Jo īpaši, attiecīgā gadījumā šādiem pasākumiem būtu jāgarantē, ka sistēmai ir iebūvēti operacionāli ierobežojumi, kurus pati sistēma nevar neievērot, un ka tā reaģē uz cilvēka-operatora virsvadību un ka fiziskām personām, kurām uzticēta šī virsvadība, ir uzdevuma veikšanai nepieciešamā kompetence, apmācība un pilnvaras. Attiecīgā gadījumā ir arī būtiski nodrošināt, ka augsta riska MI sistēmas ietver mehānismus, kas ievirza un informē fizisku personu, kurai ir uzticēta cilvēka virsvadība, lai tā pieņemtu informētus lēmumus par to, vai, kad un kā iejaukties, lai izvairītos no negatīvām sekām vai riskiem, vai apturētu sistēmu, ja tā nedarbojas, kā paredzēts.

- **Atbildība, atbilstības un ietekmes novērtēšana, uzraudzība.** Ņemot vērā augsta riska MI sistēmu sarežģītību un ar tām saistītos riskus, ir svarīgi izstrādāt pienācīgas atbilstības novērtēšanas procedūras augsta riska MI sistēmām. Saskaņā ar MI aktu pirms augsta riska MI sistēmas laišanas ES tirgū vai pirms tiek uzsākta citāda šādas sistēmas izmantošana, to nodrošinātājam jāveic MI sistēmas atbilstības novērtēšana**.** Biometriskajām sistēmām neatkarīgi no to lietojuma ir jāveic trešās personas veikts atbilstības novērtējums. Atbilstības novērtējums ir process, kurā apliecina, ka to sistēma atbilst prasībām, kas obligāti piemērojamas uzticamam mākslīgajam intelektam, piemēram, attiecībā uz datu kvalitāti, dokumentāciju un izsekojamību, pārredzamību, cilvēka veiktu pārraudzību, precizitāti, kiberdrošību un noturību. Cita starpā šī procesa gaitā ir jāizvērtē, vai augsta riska MI sistēmas ir noturīgas pret kļūdām, defektiem vai neatbilstībām. Pēc tam, kad ražojums laists tirgū, augsta riska MI sistēmu sagādātājiem jāievieš arī kvalitātes un riska pārvaldības sistēmas. Dažus pamattiesību apdraudējumus var pilnībā identificēt tikai tad, ja zina augsta riska MI sistēmas izmantošanas kontekstu. Tāpēc MI akts paredz, ka konkrētiem augsta riska MI sistēmu uzturētājiem jāveic ietekmes uz pamattiesībām novērtēšanu. Konkrētāk, šāds novērtējums ir jāveic publisko tiesību subjektiem vai privātiem uzturētājiem, kas sniedz sabiedriskos pakalpojumus, kā arī uzturētājiem, kas nodrošina augsta riska MI sistēmas, kuras veic kredītspējas novērtēšanu vai cenas un riska novērtēšanu dzīvības un veselības apdrošināšanas jomā. Novērtējuma par ietekmi uz pamattiesībām mērķis ir panākt, lai uzturētājs identificētu konkrētos riskus to personu vai personu grupu tiesībām, kas varētu tikt skartas, un identificētu pasākumus, kas jāveic minēt riska iestāšanās gadījumā. Ņemot vērā identificētos riskus, uzturētājiem jānosaka pasākumi, kas jāveic minēto risku iestāšanās gadījumā. Lai mazinātu risku pamattiesībām, varētu tikt izstrādāta, piemēram, cilvēka virsvadības kārtība saskaņā ar lietošanas instrukciju, vai sūdzību izskatīšanas un tiesiskās aizsardzības procedūras. Pēc minētā ietekmes novērtējuma veikšanas uzturētājam par to būtu jāpaziņo attiecīgajai tirgus uzraudzības iestādei. Lai nodrošinātu MI aktā noteikto prasību izpildi, ir jāizveido efektīvs uzraudzības mehānisms MI aktā noteikto prasību izpildei. ES un valstu uzraudzības iestādēm būtu jāizstrādā vadlīnijas, kas izskaidrotu, kā izpildīt MI aktā noteiktās prasības, tai skaitā kā veikt atbilstības novērtējumu un ietekmes uz pamattiesībām novērtējumu.

Izmantotie avoti

Tiesību akti

Starptautiskie līgumi un Eiropas Savienības tiesību akti

Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija. Pieņemta 04.11.1950. (EP, Latvijā spēkā no 27.06.1997.). *Latvijas Vēstnesis*, 13.06.1997., Nr. 144/145.

Eiropas Cilvēktiesību konvencija ar grozījumiem, kas izdarīti ar 11., 14. un 15. protokoliem, iekļaujot protokolus Nr. 1, 4, 6, 7, 12, 13 un 16. (neoficiāls tulkojums) https://www.echr.coe.int/documents/d/echr/convention_lav

Eiropas Savienības Pamattiesību harta. Pieņemta 07.12.2000. *OV C* 2020/239, 07.06.2016. http://data.europa.eu/eli/treaty/char_2016/oj

Līgums par Eiropas Savienības darbību (konsolidētā versija). *OV C* 326. 26.10.2012. http://data.europa.eu/eli/treaty/tfeu_2012/oj

Līgums par Eiropas Savienību (konsolidētā versija), *OV C* 115/13, 09.05.2008. http://data.europa.eu/eli/treaty/tfeu_2012/oj

Eiropas Parlamenta un Padomes Regula (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts). *OV L* 2024/1689, 12.07.2024. http://data.europa.eu/eli/reg/2024/1689/oj

Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). *OV L* 119, 04.05.2016. http://data.europa.eu/eli/reg/2016/679/oj

Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI. *OV L* 119, 04.05.2016. http://data.europa.eu/eli/dir/2016/680/oj

Eiropas Parlamenta un Padomes Direktīva 2010/41/ES (2010. gada 7. jūlijs) par to, kā piemērot vienlīdzīgas attieksmes principu vīriešiem un sievietēm, kas darbojas pašnodarbinātas personas statusā, un ar kuru atceļ Padomes Direktīvu 86/613/EEK. *OV L* 180, 15.7.2010. http://data.europa.eu/eli/dir/2010/41/oj

Eiropas Parlamenta un Padomes Direktīva 2006/54/EK (2006. gada 5. jūlijs) par tāda principa īstenošanu, kas paredz vienlīdzīgas iespējas un attieksmi pret vīriešiem un sievietēm nodarbinātības un profesijas jautājumos, *OV L* 204, 26.7.2006. http://data.europa.eu/eli/dir/2006/54/oj

Padomes Direktīva 2004/113/EK (2004. gada 13. decembris), ar kuru īsteno principu, kas paredz vienlīdzīgu attieksmi pret vīriešiem un sievietēm, attiecībā uz pieeju precēm un pakalpojumiem,

preču piegādi un pakalpojumu sniegšanu, *OV L* 373, 21.12.2004. http://data.europa.eu/eli/dir/2004/113/oj

Padomes Direktīva 2000/78/EK (2000. gada 27. novembris), ar ko nosaka kopēju sistēmu vienlīdzīgai attieksmei pret nodarbinātību un profesiju*, OV L 303,* 2.12.2000. http://data.europa.eu/eli/dir/2000/78/oj

Padomes Direktīva 2000/43/EK (2000. gada 29. jūnijs), ar ko ievieš vienādas attieksmes principu pret personām neatkarīgi no rasu vai etniskās piederības*, OV L* 180. 19.7.2000. http://data.europa.eu/eli/dir/2000/43/oj

Latvijas tiesību akti

Latvijas Republikas Satversme. Pieņemta 15.02.1922. (spēkā no 07.11.1922.). *Latvijas Vēstnesis*, 01.07.1993., Nr. 43.

Fizisko personu — tiesiska darījuma dalībnieku — diskriminācijas aizlieguma likums. Pieņemts 29.11.2012. *Latvijas Vēstnesis*, 19.12.2012., Nr. 199.

Kriminālprocesa likums. Pieņemts 21.04.2005, *Latvijas Vēstnesis*, 11.04.2005., Nr. 74.

Administratīvā procesa likums. Pieņemts 25.10.2001, *Latvijas Vēstnesis*, 14.11.2001. Nr. 164.

Darba likums. Pieņemts 20.06.2001. *Latvijas Vēstnesis*, 06.07.2001. Nr. 105.

Izglītības likums. Pieņemts 29.10.1998, *Latvijas Vēstnesis*, 17.11.1998., Nr. 343/344.

Par sociālo drošību. Pieņemts 07.09.1995. *Latvijas Vēstnesis*, 21.09.1995., Nr. 144.

Operatīvās darbības likums. Pieņemts 16.12.1993, *Latvijas Vēstnesis*, 30.12.1993, Nr. 131.

Par policiju. Pieņemts 04.06.1991. *Latvijas Republikas Augstākās Padomes un Valdības Ziņotājs*. 15.08.1991, Nr. 31/32.

Tiesību aktu projekti

Council of the European Union, Proposal for the Directive of the European Parliament and of the Council on improving working conditions in platform work, 8 March 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7212_2024_ADD_1&qid=1716971116381

Literatūra un citi materiāli

AlgorithmWatch. (13 January 2022). Fixing Online Forms Shouldn't Wait Until Retirement. https://algorithmwatch.org/en/unding-online-forms/

Ali, M., Sapiezynski, P., Bogen, M. et al. (2019). Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes, *Proceedings of the ACM on Human-Computer Interaction*, 3. https://doi.org/10.1145/3359301

Angwin, J., Larson, J., Kirchner, L. et al. (5 April, 2017). Minority Neighborhoods Pay Higher Car Insurance Premiums Than White Areas With the Same Risk. ProPublica. https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-white-areas-same-risk

Barkane I. (2023). Cilvēktiesību nozīme mākslīgā intelekta laikmetā. Privātums, Datu aizsardzība un regulējums masveida novērošanas novēršanai. Rīga: LU Akadēmiskais apgāds. https://doi.org/10.22364/cnmil.23

Barzilay, A.R., Ben-David, A. (2017). Platform Inequality: Gender in the Gig-Economy. *Seton Hall Law Review*: Vol. 47 (2). https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1588&context=shlr

Bartoletti, I., Xenidis, R. (2023). Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination, Council of Europe. https://edoc.coe.int/en/artificial-intelligence/11649-study-on-the-impact-of-artificial-intelligence-systems-their-potential-for-promoting-equality-including-gender-equality-and-the-risks-they-may-cause-in-relation-to-non-discrimination.html

BBC. (8 April 2023). Facial recognition tech: Liberty 'police racism' claim. https://www.bbc.com/news/uk-wales-65214494

Brown, L. X. Z. (16 November, 2020). How Automated Test Proctoring Software Discriminates Against Disabled Students. Centre for Democracy and Technology. https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/

Buolamwini, J., Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, pp. 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

Burgess**,** M. (6 March, 2023). This Algorithm Could Ruin Your Life. *Wired*. https://www.wired.com/story/welfare-algorithms-discrimination/

Burke, L. (13 December, 2020). The Death and Life of an Admissions Algorithm. *Inside Higher Ed*. https://www.insidehighered.com/admissions/article/2020/12/14/u-texas-will-stop-using-controversial-algorithm-evaluate-phd

Butler S. (2021). Uber facing new UK driver claims of racial discrimination. *The Guardian.* https://www.theguardian.com/technology/2021/oct/06/uber-facing-new-uk-driver-claims-of-racial-discrimination

Centre for Data Ethics and Innovation. (2020). Review into bias in algorithmic decision-making. https://assets.publishing.service.gov.uk/media/60142096d3bf7f70ba377b20/Review_into_bias_in_algorithmic_decision-making.pdf

Council of Europe, CAHAI. (2020). Feasibility Study. https://rm.coe.int/cahai202023finaleng-feasibilitystudy/1680a0c6da

Dastin, J. (11 October, 2018). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters.* https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/

De Heer, S. (25 July, 2023). A Scandal on AI in Administration, Again. *Verfassungsblog*. https://verfassungsblog.de/a-scandal-on-ai-in-administration-again/

Devlin, H. (16 February, 2020). AI systems claiming to 'read' emotions pose discrimination risks. *The Guardian*. https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks

Dutch Data Protection Authority. (2024). AI & Algorithmic Risks Report Netherlands. Report winter 2023/2024. https://www.autoriteitpersoonsgegevens.nl/uploads/2024-01/AI%20%26%20Algorithmic%20Risks%20Report%20Netherlands%20-%20winter%202023%202024.pdf

Dutch Data Protection Authority. (2023). Algorithmic Risks Report Netherlands. https://autoriteitpersoonsgegevens.nl/uploads/2023-08/Algorithmic%20Risks%20Report%20Netherlands%20-%20July%202023_0.pdf

DutchNews. (1 March, 2024). "Student finance group Duo did discriminate in fraud probes". https://www.dutchnews.nl/2024/03/student-finance-group-duo-did-discriminate-in-fraud-probes/

European Labour Authority. (2023). Artificial Intelligence and Algorithms in Risk Assessment. Addressing Bias, Discrimination and other Legal and Ethical Issues. A Handbook. https://www.ela.europa.eu/sites/default/files/2023-08/ELA-Handbook-AI-training.pdf

Feathers, T. (2 March, 2021). Major Universities Are Using Race as a "High Impact Predictor" of Student Success. The Markup. https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success

FRA. (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Gentzel, M. (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy. *Philosophy & Technology,* 34, p. 1639–1663. https://doi.org/10.1007/s13347-021-00478-z

Gerards, J., Xenidis, R. (2021). Algorithmic discrimination in Europe – Challenges and opportunities for gender equality and non-discrimination law, European Commission. https://data.europa.eu/doi/10.2838/544956

Grother, P., Ngan, M., Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8271

Hardesty, L. (11 February, 2018). Study finds gender and skintype bias in commercial artificial intelligence systems. *Massachusetts Institute of Technology.* https://news.mit.edu/2018/ study-findsgenderskintypebiasartificialintelligencesystems0212

Harwell, D. (13 April 2021). Wrongfully arrested man sues Detroit police over false facial recognition match. *Washington Post*. www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/

Heikkilä**,** M. (29 March, 2022). Dutch scandal serves as a warning for Europe over risks of using algorithms. *Politico.* https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

Henley, J. (14 January, 2021). Dutch government faces collapse over child benefits scandal. *The Guardian*. https://www.theguardian.com/world/2021/jan/14/dutch-government-faces-collapse-over-child-benefits-scandal

Hiltunen**,** R. (1 August**,** 2018**)**. Multiple discrimination in assessing creditworthiness. *European network of legal experts in gender equality and non-discrimination.* https://www.equalitylaw.eu/downloads/4658-finland-multiple-discrimination-in-assessing-creditworthiness-pdf-120-kb

Jackson I. (2024). Uber Eats worker wins payout over 'racist' AI facial recognition – what can HR learn? *People Management.* https://www.peoplemanagement.co.uk/article/1866835/uber-eats-worker-wins-payout-racist-ai-facial-recognition-—-hr-learn

Joint civil society amendments to the Artificial Intelligence Act. Prohibit remote biometric categorisation in publicly accessible spaces, and any discriminatory biometric categorization. https://www.accessnow.org/wp-content/uploads/2022/05/Amendments-to-the-AI-Acts-treatment-of-biometric-categorisation.pdf

Kayser-Bril, N. (2020). Automated Discrimination: Facebook uses gross stereotypes to optimize ad delivery, *AlgorithmWatch*. https://algorithmwatch.org/en/automated-discrimination-facebook-google/

Kippin, S., Cairney, P. (2022). The COVID-19 exams fiasco across the UK: four nations and two windows of opportunity. *British Politics*, 17, p. 1–23. https://doi.org/10.1057/s41293-021-00162-y

Knight W. (19 November, 2019). The Apple Card Didn't 'See' Gender—and That's the Problem. *Wired.* https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/

Latvijas Republikas Satversmes 91. pants. (2022). Tiesiskās vienlīdzības princips. Satversmes tiesas judikatūra. *Satversmes tiesa*. https://www.satv.tiesa.gov.lv/wp-content/uploads/2023/12/Gramatzurnals_Latvijas-Republikas-Satversmes-91.-pants.pdf

Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. *The Alan Turing Institute*. https://doi.org/10.5281/zenodo.4050457

Liang, W., Yuksekgonul, M., Mao, Y. et al. (2023). GPT detectors are biased against non-native English writers, *Patterns*, 4 (7). https://doi.org/10.1016/j.patter.2023.100779

Matzat**,** L. (21 Novembre, 2018). Finnish Credit Score Ruling raises Questions about Discrimination and how to avoid it. *AlgorithmWatch*. https://algorithmwatch.org/en/finnish-credit-score-ruling-raises-questions-about-discrimination-and-how-to-avoid-it/

Michalski, D., Yiu, S. Y., Malec, C. (2018). The impact of age and threshold variation on facial recognition algorithm performance using images of children, *2018 International Conference on Biometrics* (*ICB*), pp. 217–224. https://doi.org/10.1109/ICB2018.2018.00041

Minderoo Centre for Technology and Democracy. *(*2022*)*. A Sociotechnical Audit: Assessing Police use of Facial Recognition*.* https://www.mctd.ac.uk/a-sociotechnical-audit-assessing-police-use-of-facial-recognition/

Myers**,** A. (15 May, 2023). AI-Detectors Biased Against Non-Native English Writers. *Stanford Institute for Human-Centered Artificial Intelligence*. https://hai.stanford.edu/news/ai-detectors-biased-against-non-native-english-writers

New York State Department of Financial Services. (2021). *Report on Apple Card Investigation.* https://www.dfs.ny.gov/system/files/documents/2021/03/rpt_202103_apple_card_investigation.pdf

NL Times. (22 MAY 2024). Education agency discriminated against even more ethnically diverse students: new study. https://nltimes.nl/2024/05/22/education-agency-discriminated-even-ethnically-diverse-students-new-study

Parliament adopts Platform Work Directive. News European Parliament, 24-04-2024. https://www.europarl.europa.eu/news/en/press-room/20240419IPR20584/parliament-adopts-platform-work-directive

Radiya-Dixit, E. (2022). A Sociotechnical Audit: Assessing Police Use of Facial Recognition*.* https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf

Sample, I. (10 July, 2023). Programs to detect AI discriminate against non-native English speakers, shows study. *The Guardian.* https://www.theguardian.com/technology/2023/jul/10/programs-to-detect-ai-discriminate-against-non-native-english-speakers-shows-study

Sabbagh, D. (11 August, 2020). South Wales police lose landmark facial recognition case. *The Guardian.* https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case

Simons & Simons. (2 September, 2020). UK Court of Appeal finds facial recognition technology unlawful. https://www.simmons-simmons.com/en/publications/ckelg1z7p8kjt09008l0bet7c/uk-court-of-appeal-finds-facial-recognition-technology-unlawful

Smith, M., Mann, M. (2024). Facial Recognition Technology and Potential for Bias and Discrimination. In: Matulionyte R, Zalnieriute M, eds. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge Law Handbooks. Cambridge University Press, p. 87-95.

South Wales Police. Facial Recognition Technology. https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/

ten Seldam**,** B, Brenninkmeijer**,** A. (30 April, 2021)**.** The Dutch benefits scandal: a cautionary tale for algorithmic enforcement. *EU Law Enforcement*. https://eulawenforcement.com/?p=7941

The World Bank. (2024). AI Revolution in Education. What You Need to Know. https://documents1.worldbank.org/curated/en/099734306182493324/pdf/IDU152823b13109c514ebd19c241a289470b6902.pdf

University of Cambridge. (27 October, 2022). UK police fail to meet 'legal and ethical standards' in use of facial recognition. https://www.cam.ac.uk/research/news/uk-police-fail-to-meet-legal-and-ethical-standards-in-use-of-facial-recognition

van Es, K., Everts, D., Muis, I. (2021). Gendered language and employment Web sites: How search algorithms can cause allocative harm, *First Monday*, 26 (8). https://firstmonday.org/ojs/index.php/fm/article/view/11717/10200

Vervloesem, K. (6 April, 2020). How Dutch activists got an invasive fraud detection algorithm banned, *AlgorithmWatch*. https://automatingsociety.algorithmwatch.org/report2020/netherlands/netherlands-story/

Vigdor**,** N. (10 November, 2019). Apple Card Investigated After Gender Discrimination Complaints. *The New York Times.* https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

Wood, M. (2021). What are the Risks of Algorithmic Bias in Higher Education? *Every Learner Everywhere.* https://www.everylearnereverywhere.org/blog/what-are-the-risks-of-algorithmic-bias-in-higher-education/

Wulf, J. (2022). Automated Decision-Making Systems and Discrimination: Understanding causes, recognizing cases, supporting those affected, *AlgorithmWatch*. https://algorithmwatch.org/en/wp-content/uploads/2022/06/AutoCheck-Guidebook_ADM_Discrimination_EN-AlgorithmWatch_June_2022.pdf

Yahaya, A., Habu, J., Sani A. et al. (2024). Examining the Potential Misuse of Artificial Intelligence in Education*. Proceedings of the International Conference on Multidisciplinary Aspect of AI and IOT for Sustainable National Development.* https://www.researchgate.net/publication/378708196_Examining_the_Potential_Misuse_of_Artificial_Intelligence_in_Education